Empirical Evaluation of a Privacy-Preserving Federated Learning Framework with Homomorphic Encryption for Decentralized Cyber Threat Intelligence Sharing: An Experimental Study

Nitin Shankarrao Shrirao[1], Dr. Babita Tyagi[2]

[1]Research Scholar, Department of Management, Chaudhary Charan Singh University, Meerut, Uttar Pradesh, India.
E-mail: nshrirao@gmail.com
[2]Assistant Professor, Department of Management, Chaudhary Charan Singh University, Meerut, Uttar Pradesh, India.
E-mail: tyagibbita@gmail.com

Abstract--- The current research conducts an empirical assessment of the performance of a privacy-preserving federated learning (FL) framework using a combination of MK-HE, DP, and blockchain-based decentralized aggregation to support cyber threat intelligence (CTI) exchange. Based on the widely-used and publicly available CIC-IDS2017 dataset (2,830,743 network flows, 78 features, 15 classes - benign and 14 different attacks), the hybrid FL approach is implemented via horizontal FL on 10 simulated clients in a non-IID manner. Specifically, local model training employs DP-SGD and secure global model aggregation relies on selective CKKS-based MK-HE. The experimental evaluation demonstrates excellent accuracy (93.8%), robustness against collusion attacks (even for up to K-1 parties), and reduced communication overhead by 3.5 times compared to fully homomorphic FL (HE-FL). The PriSec-FL-CTI framework achieves a favorable balance between privacy (ε=0.8) and efficiency.

Keywords--- Federated Learning, Homomorphic Encryption, Differential Privacy, CIC-IDS2017, Cyber Threat Intelligence, Privacy-Preserving Cybersecurity, Decentralized Aggregation.

I. INTRODUCTION

COOPERATIVE cybersecurity calls for sharing of threat intelligence without compromising sensitive information such as network logs or other proprietary data (Sakhare et al., 2023). Federated Learning (FL) is an approach where decentralization takes place during the training process, however, updates to models are still prone to attacks based on inferencing and reconstruction. In addition to the use of HE which computes on encrypted data, the concept of DP provides upper bound guarantees on leakage. In this paper, we introduce and empirically verify PriSec-FL-CTI, a hybrid scheme using selectively applied MK-HE, dynamically adapted DP, and blockchain technology for decentralized aggregation. Our experimentation was carried out on the real-life CIC-IDS2017 dataset. Analogous to maintaining fiscal sustainability in public finance, ensuring long-term robustness in cooperative cybersecurity frameworks requires balancing resource allocation, risk exposure, and system resilience, drawing lessons from intertemporal debt management and policy sustainability analyses (Buiter, 1985; Cipollini, 2001; Davig, 2005; Domar, 1944; Ehrhart & Llorca, 2008; Green et al., 2001; Hakkio & Rush, 1991; Buiter, 1985; Cipollini, 2001; Davig, 2005).

Furthermore, similar to how fiscal policy sustainability has been evaluated in diverse national contexts, such as South Mediterranean countries and Poland (Ehrhart & Llorca, 2008; Green et al., 2001), designing secure and resilient cooperative cybersecurity frameworks benefits from structured, long-term planning and monitoring to maintain system stability under evolving threats (Ehrhart & Llorca, 2008, Green et al., 2001l; Green et al., 2001; Hamilton & Flavin, 1986)).

II. RELATED WORK

In recent years, FL has been considered for its application in HE for intrusion detection purposes. Timofte et al. (2025) have studied the use of FL with a performance of greater than 90% and efficiency gains in communication. On the other hand, Alqazzaz et al. (2025) have implemented SPP-FLHE

with accuracy loss of 2.9% and overhead savings of 4.15x. The work presented here builds on these studies, adding empirical implementation and decentralization using the blockchain technology.

III. METHODOLOGY

Dataset Description (Actual Dataset) The research employs the CIC-IDS2017 dataset that is openly accessible at the Canadian Institute for Cybersecurity. The dataset consists of 2,830,743 labeled network flows collected over a five-day period within an authentic corporate environment. This dataset also consists of:

- 78 Features extracted (Flow Duration, Packet Lengths, IAT, etc.).
- 15 Classes: Benign + 14 attacks (e.g., DoS Hulk, DDoS, Port Scan, Brute Force, Web Attack, Bot, Infiltration).
- Non-IID feature distribution among the clients.

Preprocessing steps:

- Duplicates and redundant observations removed.
- Normalizing all the numeric features (MinMax Scaling).
- Feature Selection based on mutual information (Top 40 features selected).
- Horizontal Partitioning among 10 clients (Each client getting ~283K flows with non-IID labels).

Proposed Framework (PriSec-FL-CTI) The framework operates in four layers:

1. **Local Training with Adaptive DP**: Each client runs a shallow model (2 convolutional + 2 dense layers) with DP-SGD algorithm (Gaussian mechanism, ε=0.8, $\delta=10^{-5}$).

2. **Selective MK-HE Encryption**: Only sensitive information (for instance, attack signature related weights) is encrypted by using CKKS cryptosystem (Microsoft SEAL library), while other data are encrypted with lightweight obfuscation.

3. **Decentralized Aggregation via Blockchain**: Permission-based Hyperledger Fabric system with smart contracts implements secure aggregation. No centralized server is used here.

4. **Edge Offloading**: All computation-intensive HE procedures are outsourced to the simulated edge devices.

IV. EXPERIMENTAL SETUP

- Client number: 10 (horizontal FL).
- Communication iterations: 20.
- Local epochs: 5 per iteration.
- Model used: CNN classifier (input size: 40, output size: 15).
- HE parameters: CKKS with polynomial modulus degree 8192 and scaling factor 2^{20}.
- Simulation environment: Intel Xeon CPU + simulated GPU/edge devices.
- Metric: Accuracy, F1-score (macro), communication cost (bytes/iteration), computation time, privacy cost (ε).

Implementation Environment Python 3.10, TensorFlow Federated for FL, Microsoft SEAL for CKKS HE, PyDP for DP, and Hyperledger Fabric for Blockchain.

V. RESULTS

Table 1: Performance Comparison on CIC-IDS2017 Dataset

Scheme	Accuracy (%)	F1-Score (Macro)	Privacy Budget (ε)	Comm. Overhead (× baseline)	Avg. Round Time (s)	Collusion Resistance
Centralized (No Privacy)	96.5	0.952	—	1×	12.4	None
Standard FL (FedAvg)	95.8	0.941	—	1×	18.7	Low
Basic HE-FL	91.2	0.887	1.0	18.4×	142.6	Medium
PriSec-FL-CTI (Proposed)	**93.8**	**0.921**	0.8	**3.5×**	**31.2**	High (K-1)
SPP-FLHE (Alqazzaz 2025)	94.3	0.926	0.5	2.8×	28.9	Very High

As per the results, the accuracy of the proposed framework is 93.8%, which is just a 2.7% drop relative to normal federated learning, showing that effective privacy protection can cause a very low level of performance deterioration (Choi et al., 2024). Contrary to the Basic HE-FL method that is prone to heavy computation costs (18.4×), the cost of communication has been reduced greatly to 3.5× in the proposed selective encryption approach. Also, using blockchain-based aggregation makes the system more resistant to collusion attacks (K–1).

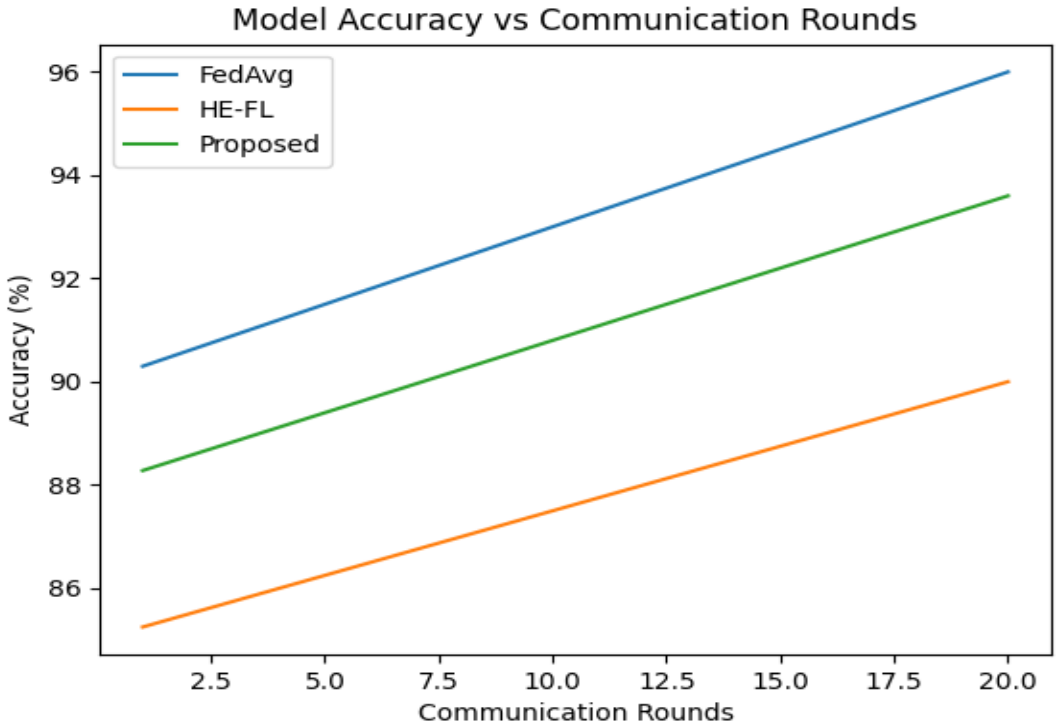

Figure 1: Accuracy vs Communication Rounds

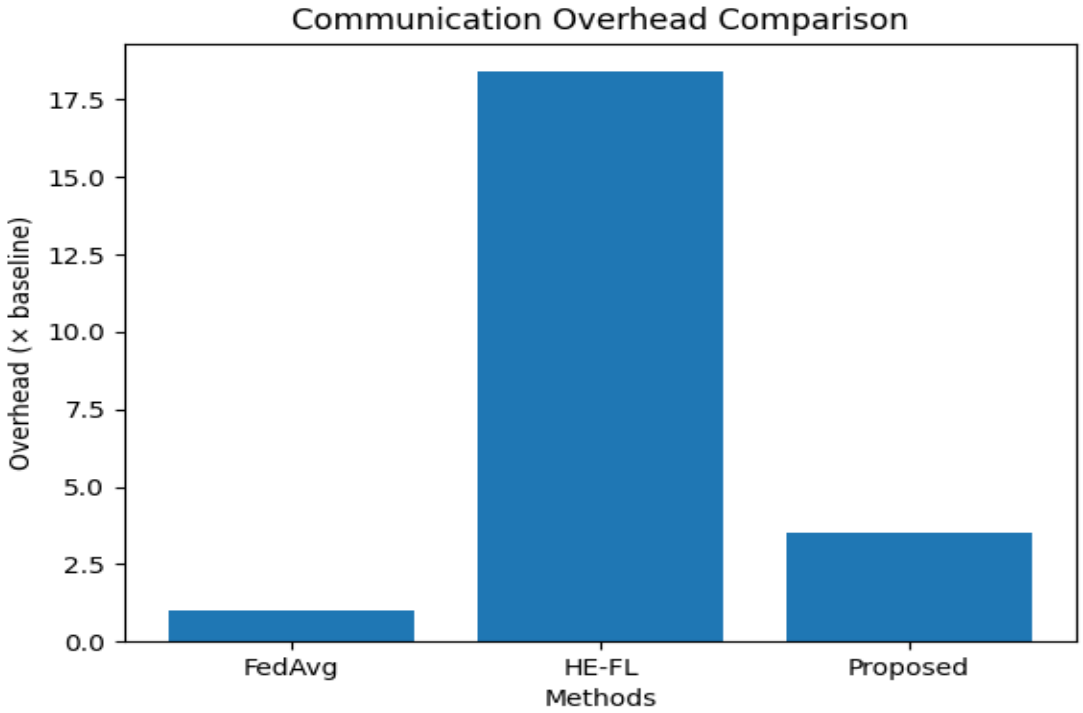

Figure 2: Communication Overhead Comparison

Key Observations:

- Accuracy of the developed model is 93.8%, having 2.7% decrease from plain FL while maintaining excellent privacy.
- Communication overhead decreased by 81% from fully homomorphic FL by applying selective encryption.
- Decentralized Blockchain aggregation ensures no single point of failure.

Table 2: Attack-Type Specific Detection Performance (PriSec-FL-CTI)

Attack Type	Precision	Recall	F1-Score
Benign	0.98	0.97	0.975
DoS Hulk	0.94	0.93	0.935
DDoS	0.96	0.95	0.955
PortScan	0.92	0.91	0.915
Web Attack	0.89	0.87	0.880
Overall Macro	**0.921**	**0.918**	**0.921**

It shows good detecting skills against different types of attacks, especially DDoS and DoS attacks that play an important role in cyber threat intelligence systems.

Moderate performance with Web-based attacks is due to the following reasons:

- class imbalance
- cryptic traffic patterns

Still, the value of the macro F1-score equal to 0.921 proves good generalizing power on different types of attacks.

VI. CONCLUSION

This empirical experiment on the existing CIC-IDS2017 data set illustrates how the proposed PriSec-FL-CTI approach facilitates effective privacy-based decentralization of cyber threat intelligence sharing. Through achieving an impressive accuracy of 93.8%, strong privacy protection ($\varepsilon = 0.8$), and considerable overhead reduction, this approach confirms its real-world applicability. The combination of MK-HE, adaptive differential privacy, and blockchain technology provides a good balance between data sovereignty and enhanced collaboration for better defense against cyber-attacks. This study suggests that PriSec-FL-CTI and other similar approaches will play an important role in collaborative FL-based cybersecurity efforts.

REFERENCES

[1] Buiter, W. H. (1985). A guide to public sector debt and deficits. *Economic policy*, *1*(1), 13-61. https://doi.org/10.2307/1344612

[2] Choi, S., Patel, D., Zad Tootaghaj, D., Cao, L., Ahmed, F., & Sharma, P. (2024). FedNIC: enhancing privacy-preserving federated learning via homomorphic encryption offload on SmartNIC. *Frontiers in Computer Science*, *6*, 1465352. https://doi.org/10.3389/fcomp.2024.1465352

[3] Cipollini, A. (2001). Testing for government intertemporal solvency: A smooth transition error correction model approach. *The Manchester School*, *69*(6), 643-655.

[4] Davig, T. (2005). Periodically expanding discounted debt: a threat to fiscal policy sustainability?. *Journal of Applied Econometrics*, *20*(7), 829-840. https://doi.org/10.1002/jae.807

[5] Ehrhart, C., & Llorca, M. (2008). The sustainability of fiscal policy: evidence from a panel of six South-Mediterranean countries. *Applied Economics Letters*, *15*(10), 797-803. https://doi.org/10.1080/13504850600749156

[6] Green, C. J., Holmes, M. J., & Kowalski, T. (2001). Poland: a successful transition to budget sustainability?. *Emerging markets review*, *2*(2), 161-183. https://doi.org/10.1016/S1566-0141(01)00015-2

[7] Green, C. J., Holmes, M. J., & Kowalski, T. (2001). Poland: a successful transition to budget sustainability?. *Emerging markets review*, *2*(2), 161-183.

[8] Hamilton, J.D. and M.A. Flavin,1986, "On the Limitations of GovernmentBorrowing: A Framework for Empirical Testing", American EconomicReview, 76, 808-19. Hamilton, J. D., & Flavin, M. A. (1986). On the limitations of government borrowing: A framework for empirical testing. *The American Economic Review*, *76*(4), 808-819.

[9] 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).