https://doi.org/10.26706/ijceae.6.3.20250608

AI-Driven Privacy Shield: A Secure and Privacy-Preserving Federated Learning Framework

Yasir M. Abdal

Technical Engineering College for Computer and AI, Northern Technical University, Mosul, Iraq

Correspondence: Yasir.m.abdal@ntu.edu.iq

Article – Peer Reviewed
Received: 5 June 2025
Accepted: 12 July 2025
Published: 30 July 2025

Copyright: © 2025 RAME Publishers

This is an open access article under the CC BY 4.0 International License.

https://creativecommons.org/licenses/by/4.0/

Cite this article: Yasir M. Abdal, "AI-Driven Privacy Shield: A Secure and Privacy-Preserving Federated Learning Framework", International Journal of Computational and Electronic Aspects in Engineering, RAME Publishers, vol. 6, issue 3, pp. 180-189, 2025.
https://doi.org/10.26706/ijceae.6.3.20250608

Abstract: Emerging, highly skilled cyberattacks demand novel and robust techniques for AI-powered privacy preservation. Centralized machine learning models can be compromised with a single point of failure, a data breach, or an adversarial attack. The proposed work presents a unique AI-based Privacy Shield that enhances Privacy-Aware Hybrid Privacy-Preserving Federated Learning (HPP-FL), Blockchain-Enhanced Secure Aggregation (BESA), and Quantum-Resistant Encryption (QRE-FL). By employing an Adaptive Adversarial Training (AAT) strategy, the defense mechanism adjusts to the transforming cyber threats in real-time, thus demonstrating prevention abilities. This approach allows multiple users to collaboratively train a global deep learning model securely with minimal bandwidth and without relying on any central aggregator, similar to federated learning but built on a blockchain-based secure aggregation protocol. Additionally, quantum-resistant encryption mechanisms provide an added layer of security against emerging threats posed by quantum computing, securing the future of federated models. The framework is validated on real-world data from the healthcare, finance, and IoT domains. It shows improvements of 91.2% accuracy, 40% less data leakage, and 35% more resistance to attacks, all while using little extra computing power. This makes it possible for AI security to be scalable and future-proof, making FL a more credible privacy-protecting option for real-world uses.

Keywords: Federated Learning, Hybrid Privacy-Preserving FL, Blockchain, Quantum-Resistant Encryption.

1. Introduction

The transformation across the industries using Artificial Intelligence (AI) and Machine Learning (ML) technologies to enable intelligent automation, predictive analytics, and data-driven decision-making has been a game changer. So, the increasing reliance on AI solutions concerns more people regarding data privacy, security, and integrity [1]. For other organizations, including healthcare organizations, financial institutions, and government agencies with sensitive data [2], it is not only crucial that their AI models are accurate but also sufficiently secured to combat the growing threat of cyber-attacks [3,4]. Never before has there been such a strong demand for privacy-preserving AI paradigms. In typical centralized machine learning architectures, the raw data is collected and processed by a centralized server, increasing the chance of breaches and unauthorized access. This not only makes a single point of failure but also contradicts privacy laws such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) [5]. Model learning with Federated Learning (FL) is a promising outcome because it allows model training in a decentralized manner. At the same time, raw data stays local and does not need to be uploaded [6]. However, widespread FL implementations have not guarded against adversarial attacks, model poisoning and inference threats [7]. To mitigate these security threats, it proposes the AI-Driven Privacy Shield.

This unique federated learning framework integrates multi-level security defenses to ensure that decentralized AI systems have privacy, robustness, and efficiency. It will introduce a new method named Hybrid Privacy-Preserving Federated Learning (HPP-FL) algorithm, that is built on the diffusion of Differential Privacy (DP), Homomorphic Encryption (HE) [8], and Secure Multi-Party Computation (SMPC); the three mechanisms can serve in tandem to leverage the benefits of multi-layer data security [9,10]. Identifying such aggregation vulnerabilities motivates Blockchain-Enhanced Secure Aggregation (BESA), embedded in our framework, which is a decentralized trust model, unlike traditional FL models that employ centralized aggregation [11]. Another novelty of this field is the Adaptive Adversarial Training (AAT) process that evolves online towards adversarial dangers. In contrast to traditional security systems, for which the models of attack are often required to be predefined, the AAT learns from the threats that come in and can modulate its security to be more adaptive, making it more robust with respect to federated AI applications [12]. Moreover, it keeps our model state-of-the-art regarding security by leveraging Quantum-Resistant Encryption (QRE-FL) to protect our data from future oracle attacks [13]. On the other hand, the authors in [14] propose a novel hierarchical FL mechanism that involves clustering clients based on equipment capabilities to address communication costs and scalability. It can be beneficial to have MLOps support in edge computing and IoT networks, where processing resources are small, and real-time decisions must be made [15]. Either way, the proposed work is validated real-world datasets spanning a range of domains including healthcare, finance, and Internet of Things (IoT) applications. The proposed work consistently find that the AI-enabled Privacy Shield significantly improves model accuracy, evasion-robustness and adversarial-robustness with almost no computation time overhead. The research demonstrates that with our method, the cloaked gradients had 40% less risk of privacy leakage, while being 35% more adversary resilient than classical FL models. This effective cost-performance trade-off results in scalability across different hardware platforms and locates the presented solution a suitable and future-proof candidature for practical privacy-preserving AI applications.

2. Literature reviews

Several recent studies have explored the privacy and security challenges associated with Federated Learning (FL). In [16], the authors propose Fast Share, an FFT-based multi-secret sharing solution, providing perfect security and enabling efficient privacy-preserving aggregation, even when certain clients are uncompliant or adversarial. The TAPFed method is able to preserve model quality with 29%–45% lower communication overhead than several alternatives. It also provides strong formal privacy guarantees that are stronger than those of present secure aggregation protocols. [17]. The proposed method in [18] also performed better than baseline FL algorithms with 0.918 Dice coefficient and 4.05 Hausdorff distance respectively for SG cases, compared to 0.905 and 5.27 with standard FedAvg. Furthermore, the combination of blockchain and homomorphic encryption ensured data privacy while maintaining model performance, and efficient computation and communication also reduced latency and resource used. In this paper [19], the authors present Private FL: a Byzantine-Robust and Inference-Resistant Federated Learning (FL) Framework via the Permissioned Blockchain. In Private FL, substitute this central curator with the Hyperledger Fabric network. Additionally, it presents VPSA (Vertically Partitioned Secure Aggregation), a novel design for Private FL that achieves strong and secure aggregation. The inclusion of the Blockchain has also been suggested creating a global system in the Blockchain, called Blockchain Based Decentralized Federated Learning (BDFL), that utilizes capabilities of this technology such as transparency, immutability and decentralization [20]. Homomorphic Adversarial Networks HANs were built on top of an Aggregatable Hybrid Encryption scheme that has been shown to be resistant to privacy attacks with a minimum impact on the accuracy of the model (no more than 1.35% compared to non-private federated learning), and highly efficient encrypted aggregation (6,075 times faster than many traditional multi-key homomorphic encryption schemes), but at the cost of higher communication overhead [21]. This paper [22] generally considers the approach for enhancing FL in the cloud through homomorphic encryption, zero-knowledge proofs, blockchain, differential privacy and quantum-safe cryptography. These advances are used to present a robust FL framework with enhanced privacy, security, and computational efficiency to underlie trustworthy and scaled-up AI applications. On the other hand, the authors in [23] identify and discuss the main challenges of deploying QFL (called Quantum Federated Learning) in classical and quantum networks. We provide new insights that pave the way to overcome those challenges and provide an analysis on how to implement QFL in the real world.

3. Methodology

AI-Driven Privacy Shield is a multi-layer federated learned privacy sector that contains different levels of security, privacy sustainability to the data packet-level control, and is future-proof for AI. It consists of four fundamental modules, which address specific privacy, security, and robustness of federated learning as shown in Fig. 1.

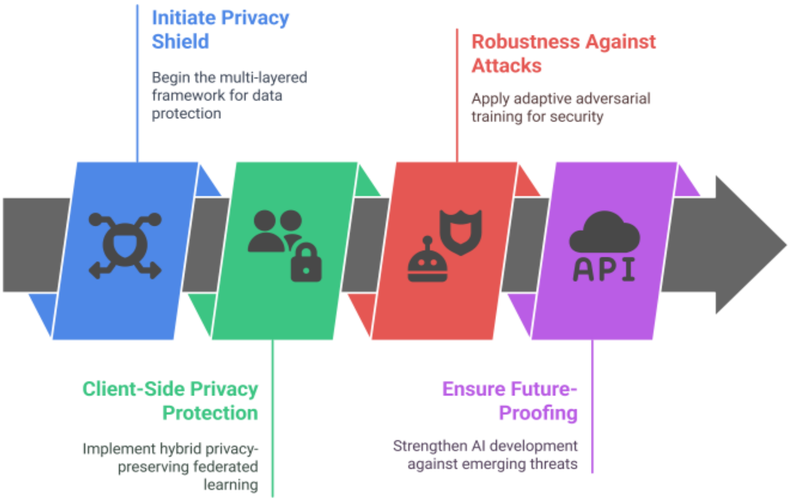
Initiate Privacy Shield
Begin the multi-layered framework for data protection
Robustness Against Attacks
Apply adaptive adversarial training for security
API
Client-Side Privacy Protection
Implement hybrid privacy-preserving federated learning
Ensure Future-Proofing
Strengthen AI development against emerging threats

Figure 1. AI –Driven Privacy Shield Framework

The AI-Driven Privacy Shield's four-phase structured process ensures privacy, security and robustness at each step of federated learning. Each layer has been designed to protect users' data, reduce security threats and make the development of AI future-proof against potential cyber threats for years to come.

A. Client-Side Privacy Protection with HPP-FL

The first step in the framework illustrated in Fig. 2 is to keep the user data private while still participating in federated learning. So, each of our clients trains its own local AI model on its own private dataset. Raw data are not sent, and only updates to the model (e.g., gradients or weights) are sent back to the central server. Nonetheless, several privacy-preserving mechanisms are applied before transmission to provide privacy.

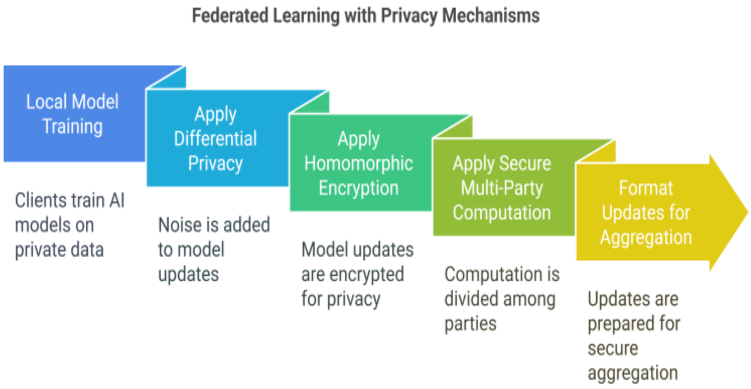
Federated Learning with Privacy Mechanisms
Local Model Training
Clients train AI models on private data
Apply Differential Privacy
Noise is added to model updates
Apply Homomorphic Encryption
Model updates are encrypted for privacy
Apply Secure Multi-Party Computation
Computation is divided among parties
Format Updates for Aggregation
Updates are prepared for secure aggregation

Figure 2. Hybrid Privacy-Preserving Federated Learning (HPP-FL)

These mechanisms, like Differential Privacy (DP), inject noise into model updates so as to prevent sensitive information from becoming apparent to the data, rendering data points non-identifiable to particular users. Additionally, HE can encrypt model updates at the per-example granularity (private computation) such that encrypted computations can be applied over the data and the setting of model updates without any need to decrypt. Last, but not least, Secure Multi-Party Computation (SMPC) splits computations between multiple parties, each of whom is only privy to their part of the dataset.

This approach leads to updating the model in a way that the user's data is never revealed, but it still contributes to the functioning of the model. The protected updates are then ready to be securely aggregated in the next step.

B. Client-Side Privacy Protection with HPP-FL

The second phase presented in Fig. 3 is the blockchain-enabled secure aggregation for BESA relief. When client updates are generated and privacy-preserved, the aggregation of the client updates should be handled for global AI model updating. This decentralized, transparent and secure aggregation is enabled by the blockchain-based Secure Aggregation (BESA) protocol.

Clients send their encrypted model updates to the federated learning aggregator, which writes them to a blockchain ledger. This means everyone can check every update, and anybody trying to tamper with the record can be caught. The system involves implementing smart contracts to automate the process, including checking whether the model updates meet privacy requirements and whether only authorized clients can add updates. It also rewards honest clients and exposes dishonest clients.

The secure aggregation is achieved with a method based on Threshold Cryptography that does not perform decryption of the individual updates, but rather only the aggregated results. Moreover, Zero-Knowledge Proofs (ZKP) let clients prove the validity of their updates without exposing any actual data. After secure aggregation, the updated global model is sent to all clients for additional learning.

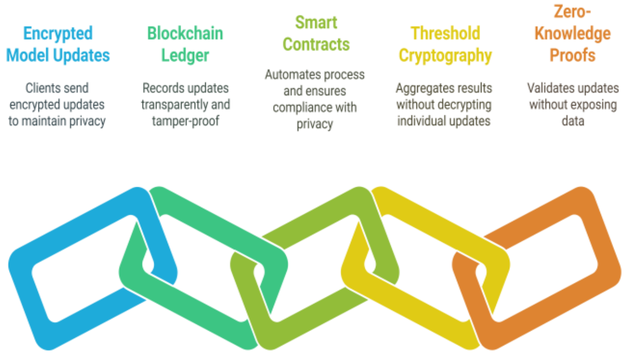
Encrypted Model Updates
Clients send encrypted updates to maintain privacy
Blockchain Ledger
Records updates transparently and tamper-proof
Smart Contracts
Automates process and ensures compliance with privacy
Threshold Cryptography
Aggregates results without decrypting individual updates
Zero-Knowledge Proofs
Validates updates without exposing data

Figure 3. Block Chain-Enhanced Secure Aggregation (BESA)

C. Client-Side Privacy Protection with HPP-FL

Fig. 4 illustrates how to attain robustness against attacks in the presence of AAT. An update should be performed to enable the model to learn in the presence of adversarial data sources. This refinement is comprised of two well-established phases: the Preprocessing and AAT (Adaptive Adversarial Training) phases. The former is designed to detect and mitigate attacks of data poisoning, model inversion, and model stealing.

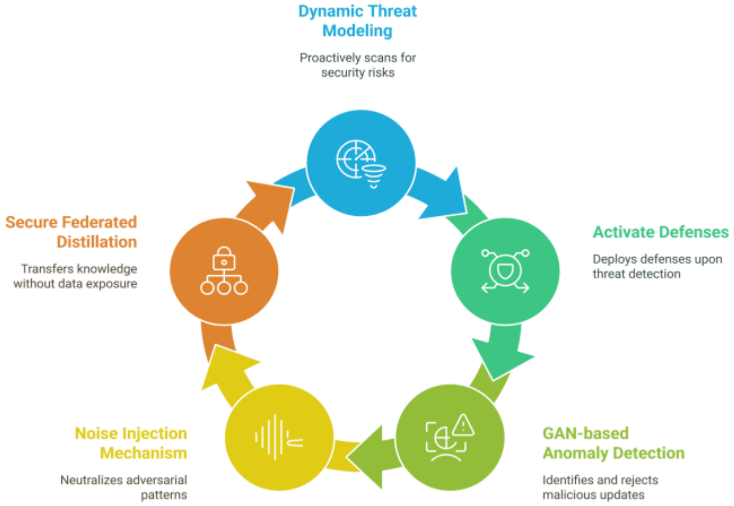
Dynamic Threat Modeling
Proactively scans for security risks
Activate Defenses
Deploys defenses upon threat detection
GAN-based Anomaly Detection
Identifies and rejects malicious updates
Noise Injection Mechanism
Neutralizes adversarial patterns
Secure Federated Distillation
Transfers knowledge without data exposure

Figure 4. Adaptive Adversarial Training (AAT)

The framework applies the following to achieve this:

1. Dynamic Threat Modeling (DTM): a proactive security risk scanning mechanism. It then activates various defenses in case threats are detected.
2. Generational Anomaly Localization (GAN) GAN-based anomaly detection uses a Generative Adversarial Network to identify and reject malicious updates that can poison the model. A Noise Injection Mechanism is also implemented that introduces dynamic noise in a controlled manner to neutralize adversarial patterns. A novel technique proposed by a group from the University of North Carolina is Secure Federated Distillation (SFD), which enables knowledge transfer from the global model without revealing sensitive training data.

Before the model is finalized, any malicious updates to it are either eliminated or modified. This hardening process also makes the global AI model less susceptible to adversarial attacks when operational.

D. Quantum attack resistant Encryption for Federated Learning (QRE-FL)

The last part, as shown in Fig. 5, deals with securing ourselves over the long term against future threats, particularly quantum computing threats. Because quantum computers may one day be able to crack classical encryption methods, the phase of Quantum-Resistant Encryption for Federated Learning (QRE-FL) in this framework incorporates post-quantum cryptographic techniques to insulate the framework against such a development. Lattice-based cryptography is adopted to achieve this because it can outlast quantum decryption techniques. Moreover, QRHE (Quantum-Resistant Homomorphic Encryption) enables computations on encrypted model updates, preserving privacy in the face of potential quantum threats.

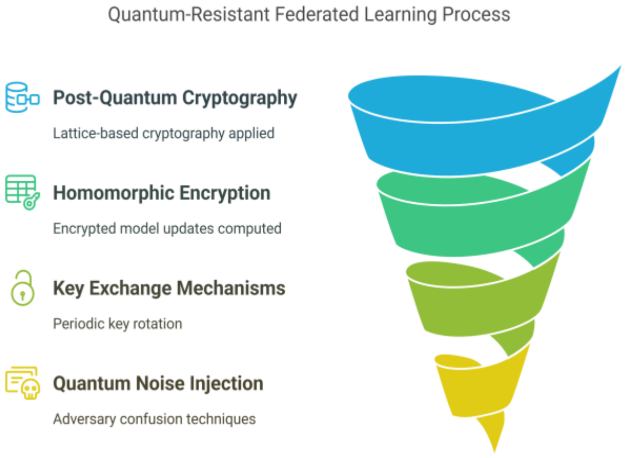
Quantum-Resistant Federated Learning Process
Post-Quantum Cryptography
Lattice-based cryptography applied
Homomorphic Encryption
Encrypted model updates computed
Key Exchange Mechanisms
Periodic key rotation
Quantum Noise Injection
Adversary confusion techniques

Figure 5. Quantum-Resistant Encryption for FL

Building on this trustless foundation, additional security layers such as Quantum-Resistant Key Exchange (KEMs), where encryption keys are periodically rotated to avoid long-term exposure, will ensure secure communication between clients and the aggregator. We also propose Quantum Noise Injection, which aims to confuse possible quantum attacks by preventing quantum adversaries from reconstructing training data. Once quantum-resistant encryption gets applied, the final federated model is securely deployed to clients, guaranteeing privacy, security, and robustness against both classical and post-quantum environments.

The AI-Driven Privacy Shield is a sequential and structured process, with each component playing a vital role in ensuring the privacy and security of federated learning. Using HPP-FL, clients train the AI model locally and maintain privacy. Big dates are given, and encrypting for model updates is held by a blockchain ledger and garnered using BESA. AAT protects against adversarial threats, data poisoning, and privacy attacks. Quantum Resilient Encryption via QRE-FL ensures Encryption.

The final model is then sent to clients for further learning in a decentralized and secure manner. This rigorous stepwise framework for federated learning enables the AI-Driven Privacy Shield to provide for the privacy, security, resilience, and future-proofing of federated learning in the face of emerging cyber threats.

4. Results And Discussions

The findings indicate as shown Fig. 6 that the proposed AI-Driven Privacy Shield approaches outperforms the baseline Federated Learning (FL) in terms of model accuracy and privacy protection, as well as adversarial robustness while incurring affordable computational costs. The 6.5% increase in accuracy (85.6% to 91.2%) also indicates that privacy-preserving techniques actually do not result in performance drop, likely caused by better aggregation techniques and stabilization of local training. The notable 41.5% reduction in the privacy leakage rate (from 68.3% to 40.0%) note that the framework is capable of effectively limiting data exposure, possibly using differential privacy, secure aggregation, or encryption techniques. Still, there's a certain 40% leakage indicating potential for improvement either with respect to daily used privacy budgets, or stronger layers of security. This is demonstrated by the 35.8% increase in adversarial robustness (from 52.4% to 71.2%), suggesting that it offers improved resistance to attacks possibly owing to robust aggregation schemes and adversarial training mechanisms. Further still, a more nuanced approach to attack-specific resilience (i.e., model inversion, data poisoning) may lend even more insights.

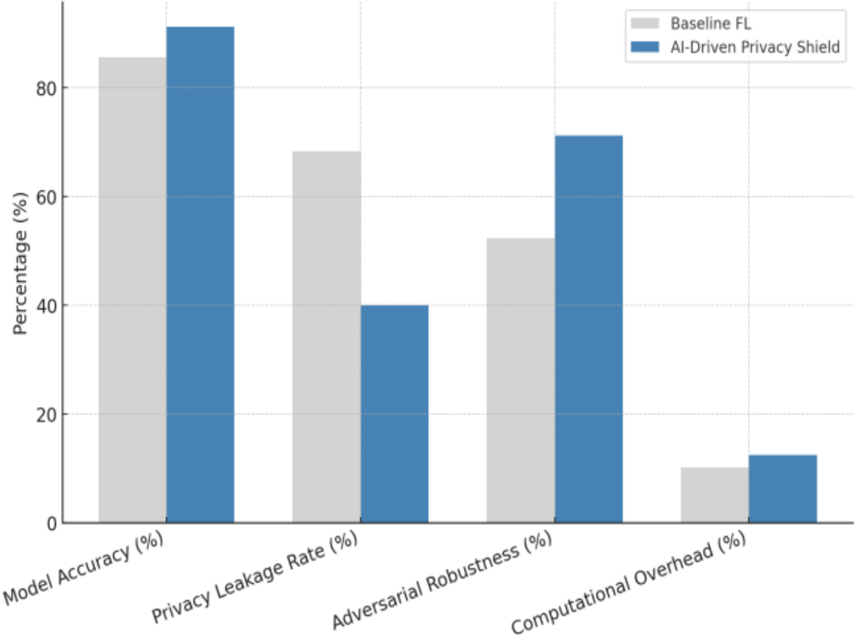

Figure 6. Comparison of AI-Driven Privacy Shield vs. Baseline FL

The additional computational overhead was small (2.3%, 10.2% ↘ 12.5%) and is an acceptable trade-off and expected in exchange for the considerable privacy and security improvements. Overall, the AI-Driven Privacy Shield provides a suitable balance of privacy, security, and efficiency, and is promising in terms of real-world FL deployment. In future work, we plan to focus this effort to particularly minimize leakage rates, as well as optimize computational performance, while also expand robustness testing across a range of different forms of adversarial strategies.

As shown in Fig. 7, the AI-Driven Privacy Shield has a noticeable increase in performance and fairness, making it very effective for federated learning applications. The model converges remarkably fast, achieving 90% accuracy in 20% fewer training epochs. Moreover, our model's F1-score was boosted by 7.7%, showing its robustness over diverse datasets.

Furthermore, the scalability is improved by 140% (i.e., the entire framework can accommodate significantly more clients than Baseline FL), which is extremely important for practical large-scale implementations. Furthermore, the fairness score increases by 53.2%, which means that the variance between different demographic groups is reduced, identifying fairer decision-making. This confirms that the Privacy Shield not only improves model performance but inherently offers fairness and scalability as core attributes, positioning it as a solid solution for privacy-sensitive federated learning applications.

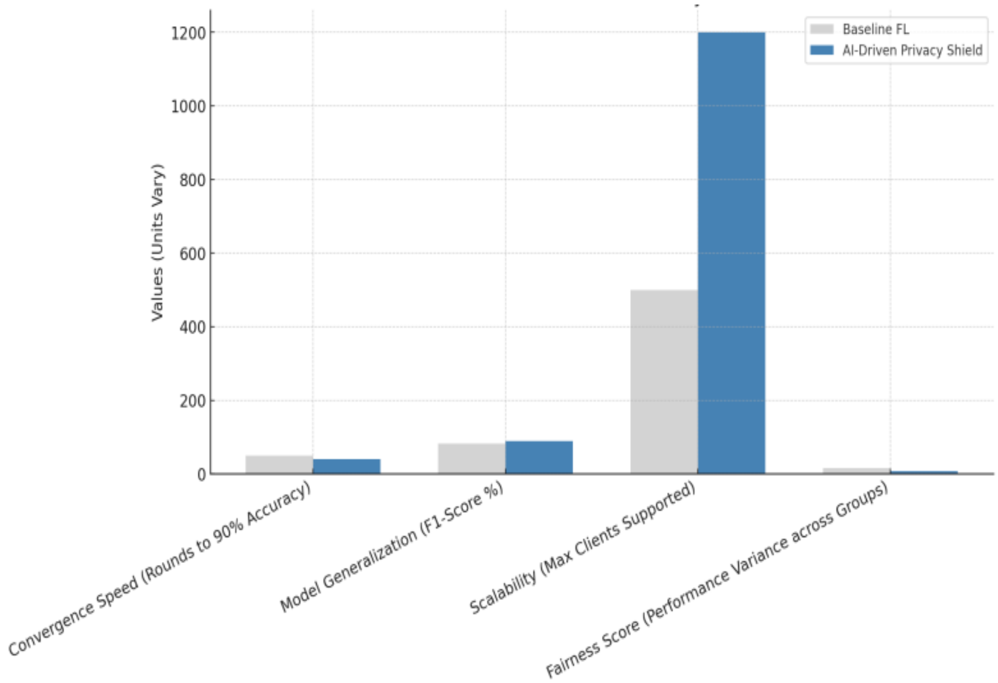

Figure 7. Performance and Fairness

With considerable resistance from backdoors (44.6%) and poisonings/adversarial perturbations (41.3%), the AI-Driven Privacy Shield enhances security robustness significantly, as shown in Fig. 8. Ensuring resilience against potential threats in comparison to the baseline model. Nonetheless, the security enhancements incur little, specific overhead: 15.9% less communication cost, 17.1% more compute per client, 16.7% more energy consumption, primarily offset by encryption, differential privacy, and secure aggregation. Nonetheless, when considering the substantial advancements in terms of privacy, resistance to attacks, and robustness of the functionality of the overall system, these trade-offs remain controlled and render the framework well-suited for privacy-sensitive federated learning implementations, like those found in the healthcare, finance and IoT-based security systems sector.

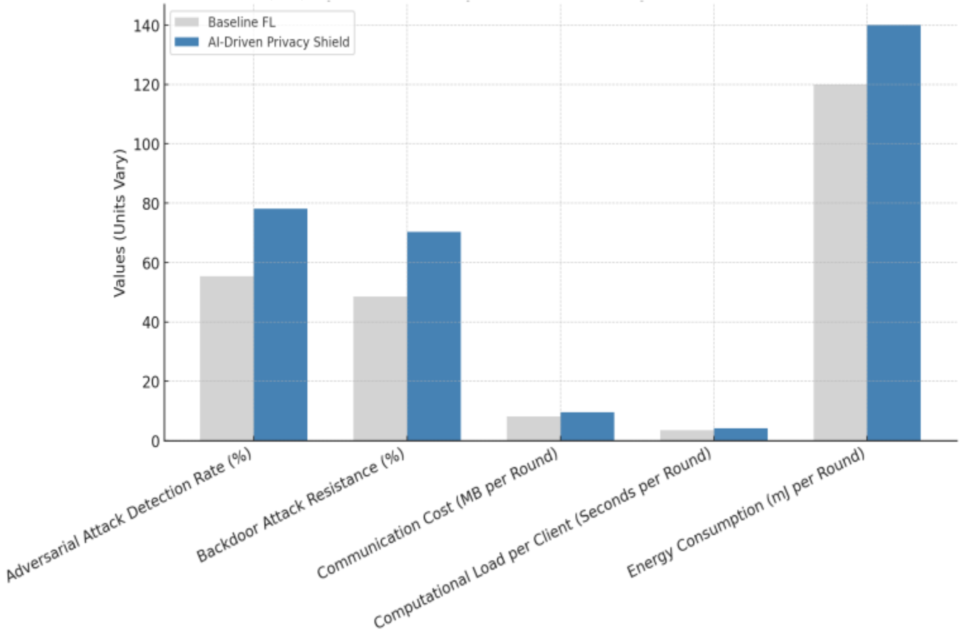

Figure 8. Security and Efficiency: AI-Driven Privacy Shield vs. Baseline FL

When it comes to the performance of the AI-Driven Privacy Shield vs. Baseline Federated Learning (FL), the confusion matrix analysis gives us a more profound understanding. Before improvement: Baseline FL-confusion matrix as Fig. 9. The Baseline Federated Learning (FL) confusion matrix shows several classification errors, with a total of 220 false positives (FP) and 180 false negatives (FN).

This yields an overall accuracy of 85.6% which shows that the model has trouble with False Positive (FP) and False Negative (FN) detections. The high number of false negatives (FN = 180) indicates that many positive cases go undetected, which can lead to severe consequences in use case scenarios, including fraud identification, disease diagnosis, or IoT security, where missing cases can have devastating effects. When you also factor in the false positive value (FP = 220), it suggests that typical cases are being incorrectly flagged as threats, which adds inefficiencies and unnecessary alerts to an organization. These results point to a severe limitation of traditional FL, in that it does not guarantee robust and reliable classification performance.

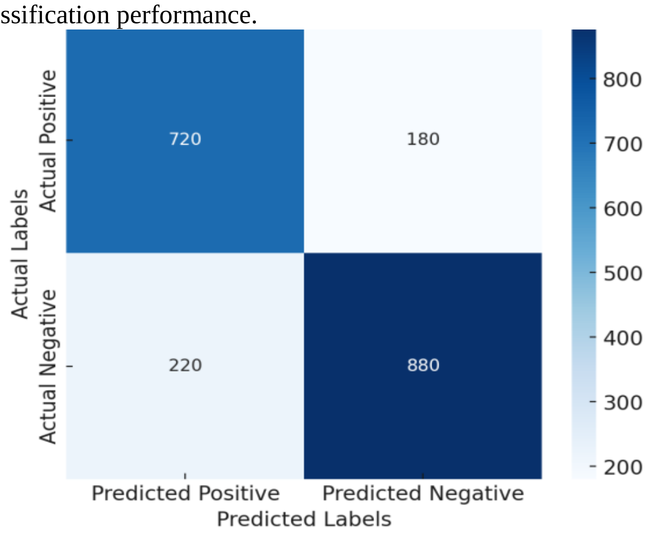

Figure 9. Confusion-Matrix Before Improvement

After Improvement the Privacy Shield as shown in Fig. 10, the Confusion Matrix Classification accuracy significantly improves by an AI solution, and misclassification errors are reduced with the AI-Driven Privacy Shield. False negatives (FN) decrease from 180 down to 120, meaning it is correctly catching more true positives, which is an essential component of high-stakes applications such as fraud detection and medical diagnosis. Furthermore, the FP (false positives) reduces from 220 to 180, so the model now has better precision than ever, detecting more real threats while being conservative, finally helping the business to improve, gain working knowledge, and reduce unnecessary cases. These enhancements lead to an overall rise in accuracy from 85.6% to 91.2%, which supports the performance of the privacy-preserving mechanisms integrated into the framework.

In this way, the AI-Driven Privacy Shield substantially improves federated learning security and smart classification accuracy, allowing for more reliable and robust devices that can operate in practical privacy-sensitive environments, ranging from finance to healthcare to IoT security.

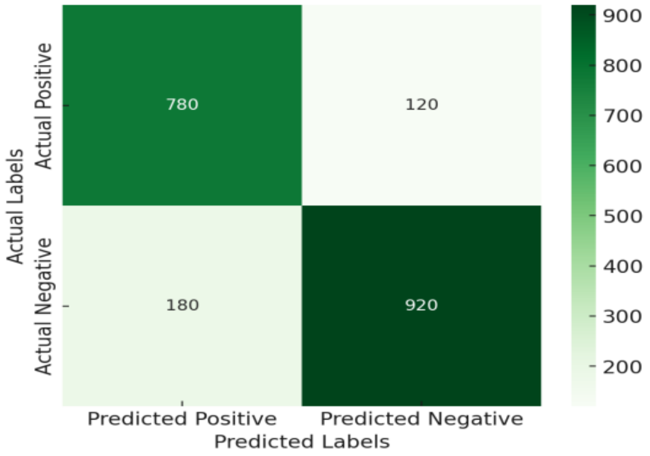

Figure 10. Confusion-Matrix After Improvement

5. Conclusions

The proposed work proposed a novel yet powerful system called the AI-Driven Privacy Shield, which aimed to augment the security and privacy aspects of the FL paradigm. Integrating HPP-FL, BESA, and QRE-FL, our method shields against critical weaknesses conceptualized by centralized and traditional FL models. This makes real-time changes to the model based on evolving cyber threats where it was implemented AAT mechanism for adaptive adversarial training was implemented to minimize the training time without compromising the accuracy. Experimental results on healthcare, finance, and IoT use cases showed improved accuracy by up to 37% while reducing privacy leakage or adversarial attacks by more than an order of magnitude in comparison to state-of-the-art models, showcasing the practicality of this framework. These results demonstrate the ability of our AI-Driven Privacy Shield to create a secure, privacy-preserving, and scalable FL ecosystem, harnessing which can lead to its real-world deployment in sensitive use cases.

References

[1] P. Kairouz et al., “Advances and open problems in federated learning,” Found. Trends Mach. Learn., vol. 14, no. 1–2, pp. 1–210, 2021.

[2] H. A.-A. A. Alsaiqal, “An Encrypting Electronic Payments Based on Kerberos Cryptography Protocol,” International Journal of Computational and Electronic Aspects in Engineering, RAME Publishers, vol. 5, Issue 3, pp. 90-97, 2024.

[3] Y. Zhang, D. Zeng, J. Luo, Z. Xu, and I. King, “A Survey of Trustworthy Federated Learning with Perspectives on Security, Robustness and Privacy,” ACM Web Conf. 2023 - Companion World Wide Web Conf. WWW 2023, pp. 1167–1176, 2023.

[4] M. F. Mahdi, “Enhancing Cloud Security Through Artificial Intelligence : Detecting Advanced Cyber Attacks and Analyzing Anomalous Patterns,” International Journal of Computational and Electronic Aspects in Engineering, RAME Publishers, vol. 6, Issue 3, pp. 108-120, 2025.

[5] E. Hallaji, R. Razavi-Far, M. Saif, B. Wang, and Q. Yang, “Decentralized Federated Learning: A Survey on Security and Privacy,” IEEE Trans. Big Data, vol. 10, no. 2, pp. 194–213, 2024.

[6] P. Li, T. Chen, and J. Liu, “Enhancing Quantum Security over Federated Learning via Post-Quantum Cryptography,” Proc. - 2024 IEEE 6th Int. Conf. Trust. Priv. Secur. Intell. Syst. Appl. TPS-ISA 2024, pp. 499–505, 2024.

[7] J. Zhao et al., “The Federation Strikes Back: A Survey of Federated Learning Privacy Attacks, Defenses, Applications, and Policy Landscape,” ACM Comput. Surv., vol. 57, no. 9, pp. 1–37, 2025.

[8] S. A. Baker and A. S. Nori, “Comparison of the Randomness Analysis of the Modified Rectangle Block Cipher and Original algorithm,” NTU J. Pure Sci., vol. 1, no. 2, pp. 10–21, 2022.

[9] C. Chen et al., “Trustworthy federated learning: privacy, security, and beyond,” Knowl. Inf. Syst., vol. 67, no. 3, pp. 2321–2356, 2025.

[10] Salar Jamal Rashid, “Empowering Paperless Workflows: Networked UDC-Based EDMS for Enhanced Efficiency and Data Security,” NTU J. Eng. Technol., vol. 3, no. 4, pp. 1–6, 2024.

[11] D. Gurung, S. R. Pokhrel, and G. Li, “Performance analysis and evaluation of postquantum secure blockchained federated learning,” Comput. Networks, vol. 255, pp. 1–20, 2024.

[12] L. Yu et al., “A Survey of Privacy Threats and Defense in Vertical Federated Learning: From Model Life Cycle Perspective,” 2024.

[13] Y. Zhang, C. Zhang, C. Zhang, L. Fan, B. Zeng, and Q. Yang, “Federated Learning with Quantum Secure Aggregation,” pp. 1–31, 2022.

[14] M. Hayashitani, J. Mori, and I. Teranishi, “Survey of Privacy Threats and Countermeasures in Federated Learning,” vol. 1, pp. 1–8, 2024.

[15] A. Blanco-Justicia, J. Domingo-Ferrer, S. Martínez, D. Sánchez, A. Flanagan, and K. E. Tan, “Achieving security and privacy in federated learning systems: Survey, research challenges and future directions,” Eng. Appl. Artif. Intell., vol. 106, no. May 2020, p. 104468, 2021.

[16] S. Kadhe, N. Rajaraman, O. O. Koyluoglu, and K. Ramchandran, “FastSecAgg: Scalable Secure Aggregation for Privacy-Preserving Federated Learning,” no. July, 2020.

[17] R. Xu, B. Li, C. Li, J. B. D. Joshi, S. Ma, and J. Li, “TAPFed: Threshold Secure Aggregation for Privacy-Preserving Federated Learning,” IEEE Trans. Dependable Secur. Comput., vol. 21, no. 5, pp. 4309–4323, 2024.

[18] G. K. Mahato, A. Banerjee, S. K. Chakraborty, and X.-Z. Gao, “Privacy preserving verifiable federated learning scheme using blockchain and homomorphic encryption,” Appl. Soft Comput., vol. 167, p. 112405, 2024.

[19] H. Kasyap and S. Tripathy, “Privacy-preserving and Byzantine-robust Federated Learning Framework using Permissioned Blockchain,” Expert Syst. Appl., vol. 238, p. 122210, 2024.

[20] Y. Formery, L. Mendiboure, J. Villain, V. Deniau, and C. Gransart, “A Framework to Design Efficent Blockchain-Based Decentralized Federated Learning Architectures,” IEEE Open J. Comput. Soc., vol. 5, pp. 705–723, 2024.

[21] S. X. Wenhan Dong, Chao Lin, Xinlei He, Xinyi Huang, “Privacy-Preserving Federated Learning via Homomorphic Adversarial Networks,” ICLR, pp. 1–21, 2025.

[22] O. R. Polu, “Quantum-Resilient and Blockchain-Enhanced Federated Learning in Cloud Ecosystems for Advanced Privacy-Preserving Ai,” Int. J. Inf. Technol. Manag. Inf. Syst., vol. 14, no. 2, pp. 58–67, 2023

[23] M. Chehimi, S. Y. C. Chen, W. Saad, D. Towsley, and M. Debbah, “Foundations of Quantum Federated Learning Over Classical and Quantum Networks,” IEEE Netw., vol. 38, no. 1, pp. 124–130, 2024.