

Postgraduate Seminar Series

Venue: Graduate Seminar Room

Date & Time: September 12, 2026 at 3:00 PM

Speaker Information

Muhammad Golam Rohman Shafi (Std No. 0424052105) is a full-time M.Sc. Engg. student in the Department of CSE, BUET. He completed his undergraduate studies in Computer Science and Engineering from Jagannath University in 2024. His research interests include Machine Learning, Federated Learning, Blockchain, and Cybersecurity. His postgraduate thesis is supervised by Dr. A. B. M. Alim Al Islam, Professor, Department of CSE, BUET. He will be speaking about his ongoing research in this talk.

A New Byzantine-Resilient Approach for Blockchain-Based Federated Learning Framework

Byzantine attack poses a critical barrier to deploying blockchain-based Federated Learning (FL) in security-sensitive domains. In a Byzantine attack, a malicious participant can implant a stealthy backdoor while maintaining the model's apparent utility on clean inputs. Existing Byzantine-resilient blockchain-FL systems often emphasize auditability and participation management. However, these existing blockchain-based FL systems still rely on single-view robust aggregation rules (e.g., distance, norm, or median-style filtering). These single-view aggregation rules are not designed to withstand modern, optimization-based, and inlier-like backdoor attacks. Therefore, going beyond single-view aggregation, this thesis presents a multi-view end-to-end Byzantine-resilient blockchain-enabled FL framework. Our framework couples permissioned multi-channel blockchain orchestration with decentralized off-chain model storage. In addition, the proposed Byzantine-resilient blockchain-based FL framework introduces a new multi-view defense mechanism — Curvature-Statistics Cross-Validation Defense (CSCVD). The proposed blockchain integrated CSCVD defense mechanism is used to detect and suppress backdoored updates while preserving clean-task performance of the proposed framework. The proposed framework is evaluated under non-IID federated settings with a standard multi-client training protocol. Experimental evaluations are conducted on three image classification benchmarks (CIFAR-10, CIFAR-100, and EMNIST) and tested against three increasingly strong backdoor threats, namely, Blackbox Poisoning, Projected Gradient Descent (PGD) backdoor optimization under update constraints, and PGD with Model Replacement (PGD+MR). Our results indicate that optimization-based stealth and model-replacement scaling cannot simultaneously bypass our proposed CSCVD's multi-view constraints. For example, on CIFAR-10 under PGD+MR attack, backdoor success is reduced to 2.76% while maintaining 88.44% validation accuracy by CSCVD. Additional evaluations highlight how the robustness behavior of CSCVD is retained under coordinated multi-attacker collusion even when attackers synchronize their malicious updates. Overall, this work contributes a new deployable blueprint for Byzantine-resilient Federated Learning by combining blockchain-based accountability with a multi-view internal consistency defense.