Researcher Profile: Dr. Mohammad Atiquzzaman  
Affiliation: School of Computer Science, University of Oklahoma

|  |  |
| --- | --- |
| Category | Content |
| Research Domains | - Federated Learning- Machine Learning- Network Security- Digital Twin (DT) Technology- Edge Computing- Unmanned Aerial Vehicle (UAV) and Unmanned Ground Vehicle (UGV)- Artificial Intelligence (AI)- Data Privacy |
| Techniques Used | - Federated Unlearning which is the safe and secure removal of data from models without entire retraining- Adversarial Machine Learning (AML) for noise generation- Deep Neural Networks (DNN) (VGG16, Resnet18, GooLeNet, DenseNet, MobileNet, ResNeXt)- Game Theory- Multi-agent reinforcement learning (MARL)- Deep reinforcement learning (DRL)- Genetic Algorithm (GA) an algorithm for optimization inspired by natural selection- Differential Evolution (DA) a population-based optimization algorithm |
| Data & Platforms | - Public Datasets: MNIST, Fashion-MNIST, CIFAR-10, Pins Face Recognition (<https://www.kaggle.com/datasets/hereisburak/pins-face-recognition)-> Models: AlexNet Model- Platforms: Python, PyTorch, AWS Cloud Computing, TensorFlow, Multi-Agent Proximal Policy Optimization (MAPPO) Framework |
| Application Areas | - Machine Learning Security- Security in 6G Networks, Vehicular Security- Smart City Surveillance- IoT Network- Healthcare- Disaster Response |

Key Research Thinking Patterns

|  |  |
| --- | --- |
| Aspect | Detail |
| Adversarial Modeling | Actively considers and develops methods to anticipate counter intelligent, malicious actions or data manipulations within systems (e.g., Data poisoning attacks in Federated Learning systems, Data privacy issues in facial recognition AI). |
| Comparative Evaluation | Assesses and contrasts various methods and systems to identify performance differences and trade-offs in metrics (e.g., Comparing Digital Twin Federated Learning Systems to already established methods, Comparing Machine Learning Facial Recognition through different Machine Learning algorithms, Benchmarked model accuracy after data poisoning). |
| Scalability Focus | Prioritizes creating solutions that are practical and efficient, being able to be implemented within larger demands or scopes (e.g., UAV and UGV architecture efficiency expanding to smart city, Unlearning as a Service being tested for larger scales). |
| AI/ML Utilization | Incorporates and develops artificial intelligence and machine learning systems within larger structures and scopes (e.g., developing Federated Learning for management systems, enabling AI-driven coordination for UAVs and UGVs). |

Knowledge Graph Sketch (Hierarchical View)

TBD

Summary Description (for use as a KG node or metadata tag)

Dr. Mohammad Atiquzzaman specializes in next-generation networking and intelligent systems. His work spans Federated Learning, network security in fields like 6G and vehicular aspects, and other applications of AI in autonomous systems like UAVs and UGVs. Notably, he introduces techniques like Unlearning as a Service for secure data removal from AI models, as well as providing more efficient solutions to UAVs and UGVs in the aspect of a smart city. Their overall contributions reflect a strong sense of comparative evaluation between current methods and their proposed solutions while also designing for larger scalability.