National Conference on Recent Trends in Engineering, Science, Humanities and Management (NCRTESHM – 2023)

29th January, 2023, West Bengal, India.

CERTIFICATE NO : NCRTESHM /2023/C0123218

ASSESSING PRIVACY-PRESERVED FEDERATED LEARNING FOR ENHANCED CYBER-ATTACK DETECTION IN EDGE-BASED IOT SYSTEMS

JITENDRA SINGH DODIYA

Research Scholar, Department of Electronics Engineering
Kalinga University, Naya Raipur, Chhattisgarh, India.

ABSTRACT

A critical challenge is the equilibrium between harnessing the potential advantages of IoT and guaranteeing strong security and privacy for consumers. Intelligent Edge Computing (IEC) emerges as a crucial answer, providing a transformative approach to data processing and security. This research presents a privacy-preserving federated learning (FL) methodology for detecting cyber-attacks in an edge-based IoT ecosystem. A unique lightweight convolutional Transformer (LCT) network is developed to accurately detect cyber-attacks by learning attack patterns from IoT traffic on local edge devices, with the model customized by fine-tuning. We assess our proposed methodology using a real-world dataset of network traffic (NSL-KDD) that encompasses many attack types, and the experimental findings indicate that our customized federated learning technique surpasses conventional federated learning. Our technique is demonstrated to be successful in managing non-stationary data and adjusting to alterations in the network environment.

Keywords: Edge Computing, Data, Privacy, Training, Precision