Intelligent, Privacy-Preserving Machine Learning Framework for Security and Intrusion Detection in Large-Scale IoT Networks – A Comprehensive Review

Jhansi Pandiri
Department of Electronics and Communication Engineering, Vignan's Foundation for Science,Technology & Research, Vadlamudi, Guntur, India

Dr. P. J. Reginald
Department of Electronics and Communication Engineering, Aditya University,Surampalem, India

Abstract

The swift growth of the Internet of Things has left a lot to be desired in terms of security with the number of devices it is getting connected to increasing and the data they generate being sensitive. Machine learning-based intrusion detection systems have proven to be a potential solution to the issue of detecting the malicious actions in the IoT environment. The study will offer a comprehensive literature survey of smart privacy-sensitive machine learning systems in intrusion detection in large-scale IoT networks. The research is conducted based on the method involving systematic literature review in the large scientific databases and analysed on the basis of the methods and strategies that preserve privacy and the approaches that identify the intrusions as well. The review presents the energy-efficient privacy-preserving methods to IoT security that are the most commonly used such as federated learning models, blockchain-based privacy models, and differential privacy models, as well as the graph neural network-based models of intrusion detection. The main theme is learning on the field of emerging privacy-preserving machine learning methods to ensure that the IoT environment is secure, and the study also reflects the current research tendencies and shortcomings.

Keywords

Internet of Things, Privacy-preserving Machine Learning, Federated Learning, Intrusion Detection System, Cybersecurity, Differential Privacy Introduction.