Short Communication
Volume 10:S1, 2021

Journal of
Telecommunications System & Management

ISSN: 2472-0437

Open Access

Artificial Intelligence-based deep learning techniques for anomaly detection in IoT using the latest IoT23 by Google's Tensorflow2.2

V.Kanimozhi

Sathyabama Institute of Science and Technology, Chennai, India

Abstract

Although numerous profound learning models had been proposed, this research article added to symbolize the investigation of significant deep learning models on the sensible IoT gadgets to perform online protection in IoT by using the realistic Iot-23 dataset. It is a recent network traffic dataset from IoT appliances. IoT gadgets are utilized in various program applications such as domestic, commercial mechanization, and various forms of wearable technologies. IoT security is more critical than network security because of its massive attack surface and multiplied weak spot of IoT gadgets. Universally, the general amount of IoT gadgets conveyed by 2025 is foreseen to achieve 41600 million. So we would like to conduct IoT intrusion and anomaly detection systems of detecting IoT-based attacks by introducing various deep learning models on artificial neural networks such as Recurrent Neural Networks, Convolutional Neural Networks, Multilayer Perceptron, Supervised GAN Adversarial Network, etc in both binary and multiclass classification modes in IoT- cybersecurity. We generate wide performance metric scores such as Accuracy, false alarm rate, detection rate, loss function, and Mean Absolute error..

Biography:

V. Kanimozhi, worked as an Assistant Professor (Computer Science) for three years and also currently working as a Data Scientist (C, C++, Java, Python, Python Libraries (Numpy, Scipy, Pandas), Machine Learning, Deep learning, Artificial Intelligence Neural Networks, Tensorflow2, Python Implementation Jupyter Notebook and Spyder3. On the verge of PhD (Data Science) in Big Data Analytics of Large Scale Network Based security and IoT using Python 3, Anaconda 3.0 & Spark Implementation in Sathyabama Institute of Science and Technology, Chennai. Published both national and international journals in Artificial Intelligence and served as an editorial board member and reviewer of international reputed journals.

Recent Publications:

1. Kanimozhi, V. & Jacob, Prem. (2021). Detailed Analysis of Top 10 AI- Deep Learning Neural Networks in Intrusion Detection for Internet of Things. 10.21203/rs.3.rs-459229/v1.
2. Kanimozhi, V. & Jacob, Prem. (2021). Artificial Intelligence for anomaly detection by employing deep learning strategies in IoT networks using the trendy IoT-23 big data from Google's Tensorflow2.2. 10.21203/rs.3.rs-364763/v1.
3. Kanimozhi, V. & Jacob, Prem. (2020). Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. ICT Express. 10.1016/j.icte.2020.12.004.