ISSN: 2393-8048
International Conference of Education New Policy Relative to Computer
Venue: Sri Vinayak Mahavidhalya, Sri Vijaynagar, Rajasthan
23 May 2019

Deep Learning-Based Anomaly Detection in Internet of Things Networks

Amit Singla, IT Head, Department of Computer Science, Seth G.L. Bihani S.D. P.G. College, Sri Ganganagar

Abstract

The rapid adoption of Internet of Things (IoT) technologies has resulted in the deployment of a large number of interconnected devices across smart homes, healthcare, transportation, industrial automation, and other critical applications. However, the increasing connectivity of IoT devices also creates significant security challenges, as resource-constrained devices and heterogeneous communication protocols can provide opportunities for malicious activities and network anomalies. This paper presents a deep learning-based framework for detecting anomalous activities in IoT networks. The proposed approach analyzes network traffic and device behavior to identify deviations from normal communication patterns. Relevant features, including packet statistics, connection duration, protocol information, traffic volume, and device-level behavior, are extracted and processed before being provided to a deep learning model. The model learns complex patterns from the training data and classifies network activities as normal or anomalous. The proposed framework can be evaluated using publicly available IoT security datasets and performance can be measured using accuracy, precision, recall, F1-score, and false-positive rate. Deep learning can reduce the dependency on manually defined detection rules and improve the ability to recognize complex and previously unseen patterns. The study also considers practical challenges such as highly imbalanced datasets, computational limitations of IoT devices, changing network behavior, and the requirement for real-time detection. The proposed framework aims to strengthen IoT network security by providing an adaptive and scalable mechanism for identifying suspicious activities.

Keywords: Internet of Things, Deep Learning, Anomaly Detection, IoT Security, Network Security, Cybersecurity, Intrusion Detection, Network Traffic, Neural Networks