IMPACT: International Journal of Research in Engineering & Technology
ISSN (P): 2347-4599; ISSN (E): 2321-8843
Vol. 12, Issue 1, Jan 2024, 1–18

DEEP LEARNING BASED APPROACH FOR DETECTING CYBER-ATTACKS IN IOT NETWORKS USING LSTM

Kuppili Shubham[1] & Rakesh Verma[2]

[1]Ph.D. Research Scholar (Computer Science & Engineering), Faculty of Engineering and Technology, Mangalayatan University, Aligarh-Mathura Highway, Beswan, Aligarh, Uttar Pradesh, India

[2]Assistant Professor, Faculty of Engineering and Technology, Mangalayatan University, Aligarh-Mathura Highway, Beswan, Aligarh, Uttar Pradesh, India

Received: 08 Jan 2024 **Accepted:** 15 Jan 2024 **Published:** 24 Jan 2024

ABSTRACT

The rapid expansion of Internet of Things (IoT) networks has transformed conventional computing environments by connecting a diverse range of sensors, smart devices, industrial controllers, healthcare systems, home appliances, and edge platforms to interconnected communication infrastructures. While this connectivity provides significant advantages in automation, real-time monitoring, and intelligent decision-making, it simultaneously creates a broad and complex attack surface for cybercriminals. IoT devices frequently operate with limited computational resources, heterogeneous communication protocols, inadequate security configurations, and constrained mechanisms for continuous monitoring, making them attractive targets for attacks such as distributed denial-of-service, malware propagation, denial-of-service, scanning, spoofing, botnet activity, and unauthorized access. Conventional intrusion detection and prevention techniques often depend on predefined signatures, manually engineered features, or static security rules, which can limit their ability to recognize previously unseen and rapidly evolving attack patterns. This study explores a deep learning-based approach for detecting and preventing cyber attacks in IoT networks by utilizing the capability of deep neural models to learn complex representations from network traffic and identify anomalous communication behavior. The proposed approach considers relevant traffic characteristics, communication patterns, packet-level information, and behavioral indicators to distinguish legitimate IoT activities from potentially malicious interactions. A structured detection framework is designed to incorporate data preprocessing, feature representation, model training, attack classification, anomaly identification, and preventive response mechanisms. Deep learning models can be evaluated according to their ability to identify multiple categories of cyber attacks while maintaining acceptable detection accuracy and minimizing false alarms. The prevention component further enables suspicious traffic or compromised communication flows to be isolated or restricted, thereby reducing the potential impact of detected attacks on connected devices and network services. Particular attention is given to the challenges of deploying intelligent security mechanisms within resource-constrained IoT environments, including computational overhead, latency, scalability, class imbalance, and changing attack behavior. The study emphasizes that combining deep learning-based detection with timely preventive responses can provide a more adaptive and resilient security architecture for IoT ecosystems. The proposed approach is expected to contribute toward strengthening continuous threat monitoring, improving attack recognition, reducing response time, and supporting the development of intelligent and scalable cybersecurity mechanisms for increasingly interconnected IoT networks.

KEYWORDS: *Deep Learning; Internet of Things; Cyber Attack Detection; Intrusion Prevention; Network Security*