Chapter 14

Intrusion Outlier Neutralizer:
A Novel LOF-Based Framework for IoT Malware Detection

Angel Justo Jones
https://orcid.org/0009-0007-9740-6611
Capitol Technology University, USA & University of Virginia, USA

ABSTRACT

The proliferation of the internet of things (IoT) has significantly enhanced the convenience and functionality of various applications ranging from personal devices to industrial systems. However, this expansion has also escalated the vulnerability of these networks to sophisticated malware attacks, posing a critical threat to the security and reliability of IoT systems. This chapter introduces an innovative defense framework based on the local outlier factor (LOF) technique for effective malware detection in IoT networks. The framework employs a systematic approach, starting from data collection and preprocessing to the application of LOF for anomaly detection. The research demonstrates through empirical analysis that the LOF-based method outperforms traditional malware detection techniques, offering higher precision, recall, and lower false positive rates. The comparative analysis with existing IoT malware detection methods such as Mobile-net IoT and Image-net IoT further validates the superiority of the LOF approach.

INTRODUCTION

In the ever-evolving landscape of cybersecurity, the detection and mitigation of malware in networked environments, particularly in the Internet of Things (IoT), remains a paramount challenge. The proliferation of IoT devices has significantly expanded the attack surface for cyber threats, making traditional security mechanisms less effective and necessitating innovative approaches to malware detection (Ahmed et al., 2016; Dhurandher et al., 2017). Recent advancements in Machine Learning (ML) and Natural Language Processing (NLP) have opened new frontiers in cybersecurity, offering sophisticated methods for identifying and neutralizing malware threats (Gubbi et al., 2013; Omar, 2018).

DOI: 10.4018/979-8-3693-1906-2.ch014

The Local Outlier Factor (LOF) algorithm, a novel approach in anomaly detection, has shown promising results in identifying aberrant patterns indicative of cybersecurity threats, including malware in IoT networks (Rostami et al., 2021; Ayo et al., 2020). Unlike traditional methods that rely on predefined patterns or signatures, LOF focuses on detecting anomalies on the basis of deviations from normal behavior, making it particularly effective against zero-day attacks and polymorphic malware variants (Venkatasubramanian, Lashkari, & Hakak, 2023; Gulatas et al., 2023).

However, the application of LOF in the context of IoT malware detection is not without challenges. The dynamic and heterogeneous nature of IoT environments, coupled with the resource constraints of many IoT devices, presents unique obstacles to the effective implementation of sophisticated algorithms like LOF (Al-Fuqaha et al., 2015; Garcia & Lewis, 2023). Additionally, the evolving nature of IoT malware necessitates continuous adaptation and refinement of detection algorithms (Victor et al., 2023).

This paper introduces ION (Intrusion Outlier Neutralizer), a novel framework that leverages the LOF algorithm for efficient and effective malware detection in IoT environments. ION is designed to overcome the limitations of traditional malware detection methods by utilizing the inherent strengths of LOF in anomaly detection while addressing the specific challenges posed by IoT ecosystems. The approach is underpinned by a comprehensive analysis of network traffic data and device behavior, using advanced machine learning techniques to distinguish between benign and malicious activities (Mall & Mishra, 2019; Xu & Wunsch, 2009).

In the ever-evolving landscape of cybersecurity, particularly in the realm of the Internet of Things (IoT), the challenge of detecting and mitigating malware continues to grow in complexity. The ION (Intrusion Outlier Neutralizer) framework represents a significant advancement in this field. Building upon the foundation laid by earlier methods such as Mobile-net IoT and Image-net IoT, ION introduces a novel approach that leverages the Local Outlier Factor (LOF) algorithm for enhanced malware detection. This framework addresses specific gaps identified in contemporary models, such as their limited effectiveness against sophisticated, polymorphic malware and zero-day attacks.

Through empirical evaluations using real-world datasets, including IoT-23 and Stratosphere IoT Dataset (Dataset Descriptions, 2023; Sgaglione et al., 2018), the researcher demonstrated the efficacy of ION in identifying and categorizing IoT malware. Moreover, the researcher compared ION's performance with existing IoT malware detection methods, such as Mobile-net IoT and Image-net IoT techniques, to prove its superior precision, recall, and adaptability in dynamic IoT environments (Kant et al., 2018; Zarpelão et al., 2017).

In summary, ION represents a significant step forward in the domain of IoT security. By harnessing the power of LOF and machine learning, it offers a robust and adaptable solution to the growing challenge of IoT malware, paving the way for safer and more secure IoT ecosystems.

LITERATURE REVIEW

Current Landscape of Malware Detection in IoT and NLP

The evolution of malware detection, particularly in the realms of the IoT and NLP, presents a multifaceted challenge. With the burgeoning the IoT ecosystem, the complexity of securing these interconnected devices has intensified (Gaurav et al., 2023; Venkatasubramanian et al., 2023). Traditional approaches like Mobile-net IoT methods, while useful, are increasingly found lacking in the face of sophisticated