2021 IEEE 18th Annual Consumer Communications &amp; Networking Conference (CCNC) | 978-1-7281-9794-4/21/$31.00 ©2021 IEEE | DOI: 10.1109/CCNC49032.2021.9369449

Anomaly Detection in Smart Environments using AI over Fog and Cloud Computing

Diego A. B. Moreira, Humberto P. Marques,
Wanderson L. Costa, Joaquim Celestino Jr and Rafael L. Gomes
State University of Ceará (UECE)
Fortaleza – CE, Brazil
E-mail: {diego, humberto, wanderson, celestino, rafaellgom}@larces.uece.br

Michele Nogueira
NR2 - Federal University of Paraná (UFPR)
Curitiba – PR, Brazil
E-mail: michele@inf.ufpr.br

***Abstract*—Modern society claims for smart environments (SEs) to make efficient the management of infrastructures, resources, and services. However, SEs comprise numerous heterogeneous devices and follow different protocols, making it harder to detect network anomalous behavior. Hence, this paper proposes ISAD, an intelligent system for network anomaly detection in SE managing Fog and Cloud computing approaches, improving the data processing and traffic exchange of the system. The system evaluation takes as workload a real network traffic, deploying locally the Fog environment and using Microsoft Azure platform as Cloud. Results show that the system detects network anomalies with an accuracy of 96%.**

***Index Terms*—Smart Environments, Machine Learning, Anomaly Detection, Edge Computing.**

I. Introduction

The Internet of Things (IoT) offers efficiency for the management of infrastructures, resources and services. IoT has been deployed combined to traditional networks, creating the concept of Smart Environments (SE). The heterogeneity in a smart environment brings novel management issues, such as *network anomalies* (i.e., a non standard behavior of network traffic) [1]. The application of proactive policies for early anomaly detection is crucial to guarantee reliability and security for services. A promising approach for Anomaly Detection in SE lies in employing Machine Learning (ML) techniques. ML techniques follow models to learn and improve the decision from experience [2]. Smart Environments tend to produce more network flows than traditional networks, due to the enormous scale of smart devices in the network, as well as the various types of applications in these devices. Hence, the monitoring of this network flows generates a high volume of data, making the application of Fog and Cloud computing essential to this scenario [3].

Within this context, this paper presents an Intelligent System for network Anomaly Detection in SE based on the integration of Fog and Cloud computing, called ISAD. Fog environment monitors SE, collects network flows (raw data), performs the processing step to identify the main features of the raw data and transmit only the useful information to the Cloud. Similarly, ML techniques work in cloud environment to dynamically define the profile of the network (i.e., the usual behavior), as well as the detection of anomalies. The goal of the proposed system lies in detecting network anomalies, while reducing the overhead.

This paper proceeds as follows. Section II describes the proposed system. Section III details the performance evaluation and results. Finally, Section IV concludes the paper.

II. Proposal

Smart Environments comprise heterogeneous smart devices, i.e., sensors, actuators, smartphones, tablets, smart TVs, smartbands, and other [4]. Each of these smart devices follows specific functionalities and, consequently, singular network behavior for a certain class/type of device.

These characteristics of smart environments increase the management complexity and, consequently, the anomaly detection in the network flows is harder. Anomalies are detected when significant changes are identified (out of the pattern) in the network profile, considering individual devices, in a group of device with similar characteristics and the network as whole. For instance, in a situation where security video cameras change drastically their behavior, increasing the size of the transmitted packets and the transmission rate, targeting an specific destination in the network or the Internet, this may indicate an anomaly related to a Distributed Denial-of-Service (DDoS) attack.

The proposed intelligent system, called ISAD, is based on the following modules: (1) *Network monitoring*, (2) *Data Processing* in the Fog, and (3) *Anomaly Detection through Machine Learning* in the Cloud. The information of the network traffic is collected in the network gateway and this raw data is sent to the Fog Environment. This raw data follows the PCAP format, which is an application programming interface (API) for low-level packet capture. It collects the information of the packets passing through the network infrastructure. The collected information includes flags in the packet header, packet size, payload size, timestamp (time that gets recorded), and others.

In the Fog environment, this raw data is processed and the useful information is extracted based on feature selection. Naturally, this processing reduces the size of the data, enabling its transmission from the Fog to the Cloud. In the Cloud environment, the behavior profile is dynamically generated

TABLE I
RESULTS OF NETWORK ANOMALY DETECTION

Metric	DT		RF		MLP	
	Accuracy (%)	Recall (%)	Accuracy (%)	Recall (%)	Accuracy (%)	Recall (%)
Scikit-learn	84.57	84	96.3	95.7	96.4	90.6
ML Studio of Microsoft Azure	91.9	75.6	98.7	83	95.86	66.95

based on features present in the data received. From this behavior profile, it is possible to detect network anomalies.

The proposed system follows the organization presented in Fig. 1, where the designed structure avails the benefits of the Fog-Cloud integration. Heterogeneous devices are connected to the network (composing the smart environment), generating multiple network flows. This network flows have different characteristics, including the destination to the Internet or among the smart devices.

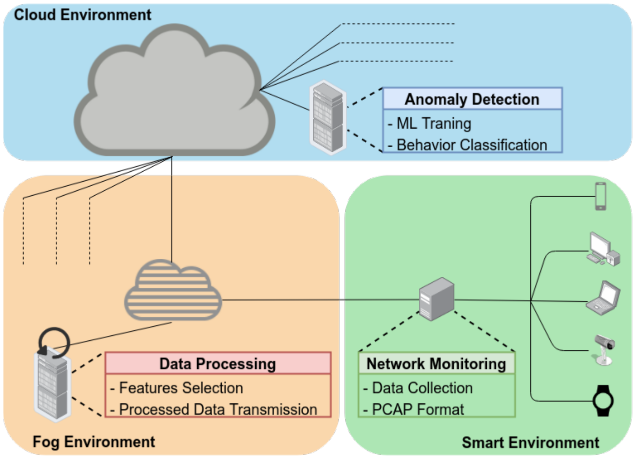

Fig. 1. Intelligent System Structure.

In Fig. 1 has three environments: Smart Environment, represented by the green box, encompasses the smart devices and the network gateway, which deploys the *Network monitoring* module; Fog Environment, depicted by the red box, is located in the edge network and the Fog node has the *Data Processing* module; and, Cloud Environment, illustrated by the blue box, instantiates a virtual machine to interact with the Fog node and to execute the *Anomaly Detection* module.

III. PERFORMANCE EVALUATION

This section presents the experiments performed to evaluate the proposed intelligent system for network anomaly detection in smart environments.

We evaluate the following ML techniques: Multilayer Perceptron Neural Network (MLP), Decision Trees (DT) and Random Forests (RF). We employ different libraries to implement ML techniques, such as Machine Learning Studio of Microsoft Azure[1] (Private platform with ML and Cloud tools) and the Scikit-learn[2] (Open-source tool in python).

The Fog environment runs in a local machine with Ubuntu Linux, CPU Intel i7-8700k 2666mhz and 16GB of Memory RAM DDR4, while the Cloud environment runs in a F48s-V2 Azure machine with 48 vCPUs and 96GB of Memory RAM. The FXXs-v2 series takes as basis the Intel Xeon Platinum 8168 processor with Turbo clock speed of 3.4GHz. The workload for experiments follows the network flows in the Intrusion Detection Evaluation Dataset (CICIDS) [5].

Table I presents the results related to accuracy and recall metrics. These results are the average of the ML techniques when both ML libraries were used (Scikit-learn and Azure ML Studio), enhancing the analysis of techniques and libraries for the problem of network anomaly detection in smart environment. We have applied a 3-Fold Cross-Validation approach in both cases. In general, the RF technique has achieved the best results, reaching 98.7% of accuracy with Azure ML Studio and 95.7% of recall with the Scikit-learn. The Azure ML Studio has presented lower recall values, indicating issues to understand several network anomalies from the normal network traffic.

IV. CONCLUSION AND FUTURE WORK

New paradigms have emerged, such as Smart Environments (heterogeneous IoT and users devices). A critical challenge in smart environments lies in the early detection of network anomalies. This paper presented a Fog-Cloud based Intelligent System for detecting network anomalies in smart environment. The system employs ML techniques to understand the usual behavior of the network flows in the smart environment, providing fast adaption to the common and sudden changes in SE network behavior. Results from performance evaluation based on real traffic as workload indicate a 86% of accuracy (in average) to detect network anomalies.

REFERENCES

[1] A. H. Hamamoto, L. F. Carvalho, L. D. H. Sampaio, T. Abrão, and M. L. Proença Jr, "Network anomaly detection system using genetic algorithm and fuzzy logic," *Expert Systems with Applications*, vol. 92, pp. 390–402, 2018.

[2] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning ddos detection for consumer internet of things devices," in *2018 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2018, pp. 29–35.

[3] F. Pisani, F. M. C. de Oliveira, E. S. Gama, R. Immich, L. F. Bittencourt, and E. Borin, "Fog computing on constrained devices: Paving the way for the future iot," 2020.

[4] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, and M. Guizani, "Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 10–16, 2016.

[5] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization." in *ICISSP*, 2018, pp. 108–116.

[1] azure.microsoft.com
[2] scikit-learn.org