AD-IoT: Anomaly Detection of IoT Cyberattacks in Smart City Using Machine Learning

Ibrahim Alrashdi
Engineering and Computer Science
Oakland University
Rochester, USA
iralrashdi@oakland.edu

Ali Alqazzaz
Engineering and Computer Science
Oakland University
Rochester, USA
aalqazzaz@oakland.edu

Esam Aloufi
Engineering and Computer Science
Oakland University
Rochester, USA
aloufi@oakland.edu

Raed Alharthi
Engineering and Computer Science
Oakland University
Rochester, USA
rsalharthi@oakland.edu

Mohamed Zohdy
Engineering and Computer Science
Oakland University
Rochester, USA
zohdyma@oakland.edu

Hua Ming
Engineering and Computer Science
Oakland University
Rochester, Michigan, USA
ming@oakland.edu

***Abstract*—In recent years, the wide adoption of the modern Internet of Things (IoT) paradigm has led to the invention of smart cities. Smart cities operate in real-world time to promote ease and quality of life in urban cities. The network traffic of a smart city via IoT systems is growing exponentially and introducing new cybersecurity challenges since these IoT devices are being connected to sensors that are directly connected to massive cloud servers. In order to mitigate these cyberattacks, the developers need to enhance new techniques for detecting infected IoT devices. In this paper, to address the IoT cybersecurity threats in a smart city, we propose an Anomaly Detection-IoT (AD-IoT) system, which is an intelligent anomaly detection based on Random Forest machine learning algorithm. The proposed solution can effectively detect compromised IoT devices at distributed fog nodes. To evaluate our model, we utilized modern dataset to illustrate the model's accuracy. Our findings show that the AD-IoT can effectively achieve highest classification accuracy of 99.34% with lowest false positive rate.**

***Keywords*—Internet of Things (IoT), smart city, Network based IDS (NIDS), Random Forest, fog layer, IoT botnet, cybersecurity.**

I. Introduction

In recent years, the proliferation of Internet of Things (IoT) has been widely increasing in societies throughout the world. The number of connected IoT devices had already reached 27 billion in 2017, and these IoT devices will exponentially increase on demand of markets, so the potential has been expected to reach approximately 125 billion in 2030 [1].

Various smart city applications connect enormous IoT devices to real-world objects, which indeed have very important benefits to urban life [2]. However, the massive number of IoT devices over heterogeneous variety types of services, technologies, devices, and protocols (e.g. Wireless, Wired, Satellite, Cellular, Bluetooth, etc.) leads to the complexity of managing future IoT networks [3], [4]. Therefore, these integration protocols with the internet leaves serious cybersecurity threats and vulnerabilities for attacking the information of the daily activities of citizen's lives. These cyberthreats can obtain unauthorized access to the IoT devices without the knowledge of either the eligible user or administrator (e.g. Miria botnet) [5].

There are two main security challenges in smart city applications. The first challenge is how to detect zero-day attacks as they happen from a variety of protocols of IoT devices in a smart city's cloud data center, assuming that the enormous attacks are hidden in IoT devices. The second one is how to find a method to intelligently detect cyberattacks [5] (e.g. IoT malware attacks, etc.) from the IoT networks before damaging a smart city. Most IoT sensors are currently gathering all of the information passing through the massive amount of data to be detected in cloud servers. Currently, traditional IDS [6] is not designed for IoT network devices, as these devices have limited resources and less functionality (e.g. smart watches, smart lamps, smart locks, etc.).

Fog computing is recently designed between cloud and IoT layers to reduce energy consumption, storage, and latency. Moreover, it aims at moving the computing process near the sensors to quickly respond to the IoT applications in a wide area, such as a smart city [7], [8]. Recently, authors in [9] suggest enhancing the detection of IoT cyberattack in the distributed fog layer. The detection in the IoT networks would be more significant to automatically alert the Internet Service Providers (ISPs) or administrators, when quickly and effectively detecting compromised IoT devices in the fog layer and interrupt the connection of the IoT attacks from the network of urban life.

In this paper, we propose the AD-IoT system which uses an intelligent anomaly detection method based on machine learning algorithms that can detect attacks with reducing the false positive rate. The AD-IoT system is also designed to monitor all IoT traffic in a distributed fog layer and alert the administrator or the provider services in a smart city. This approach can detect a challenge of hidden compromised

978-1-7281-0554-3/19/$31.00 ©2019 IEEE

IoT devices in the large scale detection in cloud computing [3], [10]–[12]. Therefore, this system is based on applying a training model in the distributed fog networks as learning intelligently from training in distributing small scale network traffics near to IoT sensors and differentiating from normal and abnormal behaviors in the future.

The contributions of this paper are as follows:

- We propose the design intelligent detection system called AD-IoT to detect and alert (e.g. administrators, Industrial management, ISPs, etc.) for detecting IoT cyberattacks or unusual activities in IoT network traffics from the fog networks distributed over the smart city (e.g. routers or switches).
- Most previous experimental works for detection on IoT malicious behaviours using IDS based on signature method based on cloud center to detect only known attack. However, in this paper, we use anomaly detection based fog network using machine learning methods to identify attacks by extracting statistic measurement on the dataset including modern attack features [13] that assumed in the IoT botnet network traffics environment [14].
- We evaluate the proposed framework system using classification Random Forest (RF) algorithm to predict benign or malicious data.

The rest of this paper is structured as follows. Section II illustrates related work. Thereafter, Section III provides information on some relevant terms regarding smart city such as its benefits, architecture, and Intrusion Detection System (IDS). Section IV discusses the threat model in a smart city and research challenges. We describe the AD-IoT system model in Section V. Section VI evaluates the method system. Section VII discuses the result and provides the future plan of this work. Finally, Section VIII concludes this work.

II. Related Work

This section presents previous studies that relate to this work on IDS in IoT network, IoT cybersecurity threats and network behavior anomaly detection based on machine learning algorithms in IoT network.

Previous studies that discuss traditional IDS methods as illustrated in section III-C have been indicated to detect cyberattacks in different ways in the host-based IDS (HIDS) [15], [16], network-based IDS (NIDS), or hybrid IDS [6], [17], [18]. Therefore, this paper relies on using NIDS anomaly-based method [7], [9], [19]–[21]. There are several techniques which rely on signature-based methods, however, this method consumes power and fails to detect novel attacks, and only detects attacks when matched with the database stored [22]. This database is not significant with low capacity in IoT devices as signature-based methods cannot detect unknown attacks in the network traffics.

Most early studies as well as current work that focuses on analysis network traffic have not concentrated on the fact that the IDS for IoT network is different from the traditional IDS. Therefore, a recent survey [6] showed that some IoT networks face difficulty with the traditional IDS methods due to some of IoT limited resources, specific protocols, consuming energy etc. IDS methods should be enhanced for IoT security services to protect their eligible users in a big infrastructure smart city [10].

Several studies have been conducted to investigate IDS for IoT networks, and the recent survey was not mentioned anomaly detection based on machine learning particularly on RF [6]. Recently, the authors in [9] have not used anomaly detection method, and utilized deep learning approach for detecting cyberattacks in fog nodes but evaluated their investigation in NSL-KDD dataset [21] which is lack of modern attack behaviors and has high performance and efficiency [23]. Furthermore, the recent work of [14] are closer to the AD-IoT approach, so they applied machine learning algorithms to detect IoT botnet with using UNSW-NB15 dataset. They differ from our approach by utilizing ARM, ANN, NB, and DT.

To the best of our knowledge, no prior researches have examined this method AD-IoT which differs from previous studies. Most of the above-mentioned existing IDS approaches do not investigate the smart city. Furthermore, this model learns from normal traffic by training machine learning algorithm such as RF algorithm to detect any malicious behaviour in the future.

III. Background

This section provides relevant background information on smart city architecture, benefits of a smart city, and intrusion detection system.

A. Smart City Overview

A smart city incorporates and uses IoT technology, smart systems, Big Data analytics and information and communication technologies to improve the quality and performance of the different services within a city. The aim of smart city is to enhance health and safety of the city dwellers, control of pollution as well as reducing wastage of resources, resource consumption, and the overall costs. The idea of a smart city improves the quality of living for the city residents through smart technology [24].

Who cares about smart city? It is the responsibility of the government to take care of the smart city by ensuring the systems are not vulnerable to cyberattacks and the privacy of the residents is guaranteed.

B. Smart City Based on Fog Architecture

Smart city architecture is based on the advantage of fog computing to reduce the latency between cloud and IoT sensor as shown in Fig. 1. It comprises of three layers for showing high view levels in smart city infrastructure [7]–[9], [12] that include application layer, fog layer, and IoT sensor layer. The fog layer is a major component of the smart city architecture, which ensures processing and aggregation of the data.

1) Cloud Layer: it contains servers to store and manage a huge amount of data at the top level management.

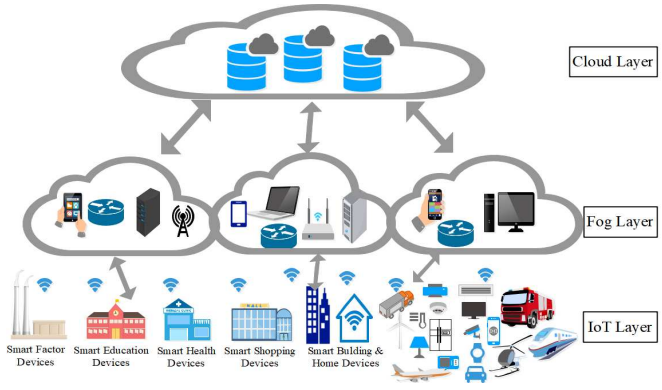

Fig. 1. Smart city based on fog architecture.

2) Fog Layer: it bridges the gap between sensing and cloud layer to make the computational and management in the edges of the network (e.g. security gateway). Distributed attack detection in fog networking is more significant than the centralized cloud layer.

3) IoT Sensing Layer: it comprises a set of sensors that are installed within the city to enable data collection.

C. Intrusion Detection Systems

Traditional IDSs are designed to monitor and detect any intrusion activities on each singular computer or on whole network traffic. There are two types of IDSs: first is *Host-based IDS (HIDS)* and second is *Network-based IDS (NIDS)*.

HIDS installs the software (e.g. anti-virus) on each computer to monitor and detect any malicious activities of the traffic intrusion behaviors based only on this computer system that connected on the traditional local network [15], [16]. HIDS can analyze or scan (e.g. application logs, system calls, file systems, etc.) the software that is installed on the computer. Thus, this HIDS method is not significant with some IoT devices such as smart lamps, watches, lock-doors, etc., that have limited functionality and resources (e.g. energy consumption, latency, computation, low memory, etc.).

NIDS monitor entire network traffic and can detect known or unknown attacks based on a hybrid method which has both signature-based and anomaly-based techniques [6], [19], [25]. The anomaly-based NIDS methods are more significant for monitoring network traffic and detecting new attacks. Even the anomaly-based method has high false positive rates; the proposed design system AD-IoT promises to reduce the false positive rates. However, signature-based would cost computation in storing attacks in database and furthermore would not detect a new attack in the future network traffics [6].

Therefore, the AD-IoT intelligent detection system promises to detect attacks by using NIDS method for anomaly-based on machine learning methods.

IV. Problem Statement

This section analyzes the threat model of IoT cyberattacks and research challenges. IoT devices have been growing exponentially with multiple heterogeneous devices. This leads to increased IoT vulnerabilities (e.g. zero-day attacks, botnets, etc.) to serve attack vectors who can target the IoT victims and use them to steal personal information, or launch DDoS attacks over the Internet [5], [26], [27]. For instance, IoT botnets can be simpler to compromise the vulnerable IoT devices by scanning the internet and finding the victims IoT network IP address. The phenomenon of the Mirai botnet happened in late 2016 when it compromised a massive amount of IoT devices by launching a DDoS attack against Dyn, which is a DNS provider [5]. Therefore, building these IoT systems can take years but crashing them takes merely days.

The main challenges for securing IoT devices may become IoT botnets without notice from the ISPs and eligible users. We consider that there are increasing security issues in most smart home networks, as they were designed with vulnerable and poor security techniques since some companies need profit or have little expertise in the security field [28]. The main security issues of massive IoT devices are built in heterogeneous types of devices and protocols that are very complex to secure in a smart city [11]. Therefore, most IoT networks are not satisfied with traditional IDS systems which would not accurately detect the IoT attack networks [6].

A. Adversary Model

We consider the adversary model that the attacker can scan the internet to compromise the vulnerable IoT devices that connect to different routers in the smart city, such as homes, hotels, restaurants, malls, airports, and so on. Thus, the attacker compromising these IoT devices can significantly gain sensitive data such as credit card information, stream video, send spam, etc. These issues would be very challenging to detect the compromised IoT devices from the huge data in the cloud center for smart city devices.

The goal of this paper proposes the AD-IoT system to identify infected IoT devices on the distribution of fog networks instead of centralized cloud computing.

B. Research Challenges and Assumptions

1) Limited Resources: Using traditional IDS method can detect the compromised computers, laptops, or smart phones on the traditional local network. However, the IoT device applications face challenges, as these IoT devices have a weak functionality. These IoT devices are very challenging as there are limited resources (e.g. small memory, batteries).

2) Heterogeneous: IoT devices are connected with various protocols. Thus, increasing IoT devices in the future in big infrastructure smart cities would cause serious damages and latency detection with massive IoT data in the cloud centers in the urban life.

3) High False Positive Rate: With using anomaly detection method, it can easily be high false positive rate. AD-IoT approach has to reduce the false positive rate.

Furthermore, we consider assumption that a massive of heterogeneous IoT devices are connected in the big smart city. AD-IoT system promises to intelligently detect zero-attacks and IoT botnets in distributing detection in the fog layer.

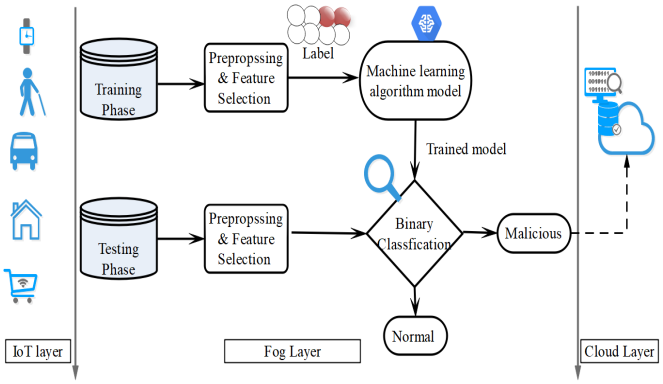

Fig. 2. Proposed AD-IoT detection system model.

V. Methodology

In this section, we propose a detection method system called AD-IoT for detecting cyberattacks at fog nodes in a smart city as illustrated in Fig. 2. The framework of this method relies on different machine learning algorithms to enhance the efficiency of AD-IoT for detecting attack behaviors in future urban IoT networks. We suppose this method works to monitor the network traffic that passes through each fog node, as fog nodes are nearest to IoT sensors, rather than detection on the huge amount of the city's cloud storage to identify among normal and abnormal behaviors. After detecting attacks in the fog level, it should alert the security cloud services to inform them to analyze and update their system.

A. System Design

This AD-IoT system design model is supposed to consist of several components involving a massive amount of IoT devices connected to distributed fog networks privately (e.g. smart home's gateway) or publicly in a smart city. Detecting from this intelligent model distributed at each fog node, it should detect the new attacks to alert the cloud server managements as described in the following:

1) IoT Devices: A massive amount of IoT devices are connected to gateway in fog layer.

2) Gateway: We suppose each private facility that has its own gateway (e.g. smart homes, buildings, malls, schools, etc.) is connected to the master AD-IoT security gateway in the fog layer to handle several gateways.

3) AD-IoT Security Gateway IDS System: It can be placed on a master fog node that can intelligently monitor the communication among the network traffic data. AD-IoT system is based on ensemble methods, which are used to improve the performance of algorithms in this system model. We choose from these methods bagging techniques which are Random Forest (RF) and Extra Tree (ET). These techniques have massive decision trees. These methods are used to train part one of the UNSW-NB15 dataset in this preliminary model and split nodes chosen by using ExtraTreesClassifier to reduce a importance selection to 12 features.

TABLE I
Traffic distribution in Multi-classification of UNSW-NB15.

Traffic	Training	Total Records
DoS	816	1167
Worms	16	24
Generic	5265	7522
Backdoors	373	534
Analysis	368	526
Fuzzers	3535	5051
Shellcode	156	223
Reconnaissance	1231	1759
Exploits	3786	5409
Attacks	15546	22215
Normal	50000	677719
Total	65546	699934

B. Anomaly Detection Based on Machine Learning

As illustrated in section IV, cyberattacks can find the vulnerable IoT devices either in private or public networks in urban life. NIDS can utilize machine learning algorithms (e.g. Decision Tree, K-Nearest Neighbor, Random Forest, etc.) to classify and detect malicious behavior in the IoT fog networks. This can be done by applying the NIDS system through use of the anomaly detection method based on machine learning algorithms, which uses statistical analysis to clean and prepare data for an intelligently predictive model. This model can identify normal traffic and abnormal attacks with reduced False Positive Rates (FPR).

Thus, this AD-IoT approach can enhance the performance for effectively detecting the attacks in fog nodes in smart city infrastructure, rather than detecting in the cloud center. As such, these IoT fog networks would guarantee a lightweight feature, less latency, and lower consumption than the cloud center, which has a massive amount of data in a big infrastructure smart city.

VI. Evaluation and Experimental Results

This section presents the analysis and evaluation of our proposed framework, AD-IoT, on different parameters which relies on the UNSW-NB15 dataset [13]. This study evaluated machine learning algorithms to identify benign network traffic from malicious activities to apply the final model on fog nodes in the AD-IoT approach in future work.

Therefore, this evaluation relies on anomaly detection which is based on the machine learning approach. More details are listed below as the following:

A. Dataset Descriptions

The UNSW-NB15 dataset was introduced in 2015 [13] to address the issue of the lack of modern normal and attack network traffic. When evaluating NIDS based on anomaly detection method in the dataset of KDD99 and NSL-KDD, it does not show the real performance. Therefore, the UNSW-NB15 includes 49 features and nine attack classifications to update the realistic benign traffic and the malicious behaviors. The authors split their dataset from several types of attacks and normal traffic to reduce the huge size of 175,341 archived records for training and 82,332 records for testing [23].

In this paper, we selected one part of the UNSW-NB15 dataset. The first step was to replace this dataset on data frame by using a Pandas library, which group features as nominal, integer, float, and binary. Meanwhile, pre-procssing (e.g. read, split, convert, normalize) then saved it to HDF5 to enhance the the massive amount of network traffic. In the second step,while reading the pre-processed data from HDF5, it split data for training 65546 sets into a newly cleaned dataset for the RF model, which contains the total of 699,934 instances and several features as shown in Table I. The RF has two classifications, normal or attack, and we chose the maximum value for training ET (15 estimators) in RF which is 50000 for normal training data. Finally, we selected features to reduce the size after vectorizing the dataset to 12 features by using ExtraTreesClassifier, which chose the most important for identifying the benign or malicious behaviour. We used random seed for each training data.

These selected features are named: *srcip, dstip, dur, dsport, ct-dst-src-ltm, ct-srv-dst, ct-dst-ltm, ct-src-ltm, ct-src-dport-ltm, dbytes, proto, and is-ftp-login.* To utilize the ExtraTreesClassifier class, it imports from calling scikit-learn (e.g. *from sklearn.ensemble import ExtraTreesClassifier*) [29].

$$\begin{aligned} Accuracy &= \frac{TP+TN}{(TP+TN+FP+FN)}, \\ FPR &= \frac{FP}{(TN+FP)}, DR = \frac{TP}{(TP+FN)} \end{aligned} \tag{1}$$

B. Evaluation Metrics

Preliminary, this work tested only AD-IoT model in the binary classification which classified as normal or attack. The evaluation metrics [30] are to detect attacks in binary labeled classifications, as shown in equation (1). To gain the result of this equation, the Accuracy shows the percentage of whole normal and attack data that can be correctly classified. To illustrate the percentage of correctly detected attack, we used Detection Rate (DR). However, to show the percentage of the incorrect detection of attack behaviors, we utilized the False Positive Rate (FPR). Thus, Accuracy showed in the result 0.99.34% to declare the percentage of true detection. FPR showed 0.02%, DR was 0.82% where True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN).

$$Precision = \frac{TP}{(TP+FP)}, Recall = \frac{TP}{(TP+FN)} \tag{2}$$

This paper measures the system model to present interim results by using confusion matrix and other metrics (e.g. precision, recall, f1-score) to find the accuracy and correctness of proposed model. First, the efficiency of using the proposed AD-IoT for detecting cyberattacks is shown by evaluating the confusion matrix to count correctly and incorrectly detected instances in actual normal records. This is shown with normal as TN, and attack as FN. However, actual attack records show FP as normal, and TP as attack as shown in Table II, and in Fig. 3 to present the confusion matrix for Random Forest.

TABLE II
CONFUSION MATRIX.

Actual	Predicted Normal	Predicted Attack
Normal	TN	FP
Attack	FN	TP

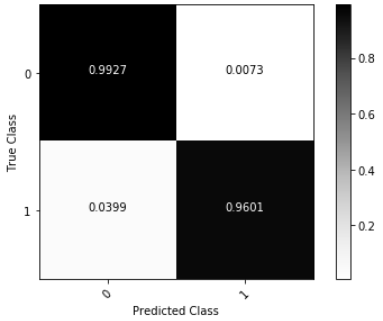

Fig. 3. Confusion matrix for RF test.

Second metrics, as we suppose the preliminary result for measuring the efficiency of performance metrics for AD-IoT in detecting the attacks at this proposed model, to distribute in fog nodes as given in precision and recall in equation (2). The precision metric shows how many of the detected malicious behaviors are correct, and the recall metric illustrates how many of the malicious attacks the model detects. Furthermore, f1-score metrics can gather both precision and recall metrics to show the average, as show in Table III. This is illustrated by using the ExtraTreesClassifier implements superior by choosing data. However, precision is still lowest in detection the attack with 0.79%, and recall is better with 0.97%.

This approach was implemented using python programming language with using libraries (e.g. Pandas, Numpy, sklearn, etc.) on a windows OS with an Intel core i7 processor and 8GB of RAM.

We plan to measure the evaluation and performance metrics by multi-classification and the performance metrics in the final model in the future work with more machine learning algorithms as discussed in the next section VII.

VII. DISCUSSION AND FUTURE WORK

This paper explains a conceptual framework for the designing AD-IoT system by using NIDS method to detect the IoT cyberattacks in a smart city. In order to illustrate a real-world example that serve as a basis for our concept study, we present this work to motivate the framework AD-IoT in a smart city. This proposed design does not yet finalized the

TABLE III
PERFORMANCE OF BINARY CLASSIFICATION.

Model	Predicted	Precision	Recall	F1-Score
RF	Normal	0.99	0.99	0.99
	Attack	0.79	0.97	0.86
	Avg/total	0.98	0.98	0.98

machine learning model and not yet account for urban life network designs.

We plan to continue developing the final model with more classification algorithms such as Conventional Neural Network (CNN), etc., to the proposed design AD-IoT system for IoT devices in a smart city. This work plan would lead to train final model parallel distributed among fog nodes and centralized the IDS in a master fog node to detect cyberattaks and identify normal or attack traffic activities in urban life. Furthermore, this work tests only the proposed preliminary model to classify the network traffic, and thereafter we will continue to distribute IDS and compare the final model based on fog network detection systems. To achieve our goal for detecting IoT attack networks in a smart city, we also plan to use open sources of distributed computing (e.g. Apache Spark, etc.) to distribute the model in fog nodes for detecting the cyberattacks and handle huge amount of data passing through the final model detection. Therefore, the beyond-work goal is to use n-fold cross validation to evaluate the performance metrics of the design AD-IoT system to increase the effective detection rates, and reduce overfitting and false positive rates.

VIII. Conclusion

The vision of a smart city security detection system is studied in this paper as efficiently enhancing a traditional IDS for smart city's IoT applications. We introduced an approach based on NIDS called AD-IoT system to detect various IoT attacks in a distributed fog layer instead of a cloud layer. The proposed AD-IoT can significantly detect malicious behavior using anomalies based on machine learning through the evaluation of the UNSW-NB15 dataset to detect the binary labeled classification before distributing on fog nodes.

References

[1] J. Howell. Number of connected iot devices will surge to 125 billion by 2030, ihs markit says - ihs technology. [Online]. Available: https://technology.ihs.com/596542/, last accessed: 11/07/2018.

[2] E. Borgia, "The internet of things vision: Key features, applications and open issues," *Computer Communications*, vol. 54, pp. 1–31, 2014.

[3] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the internet of things: New perspectives and research challenges," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 1–14, 2018.

[4] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, 2014.

[5] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis *et al.*, "Understanding the mirai botnet," in *USENIX Security Symposium*, 2017, pp. 1092–1110.

[6] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in internet of things," *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, 2017.

[7] J. Santos, P. Leroux, T. Wauters, B. Volckaert, and F. D. Turck, "Anomaly detection for smart city applications over 5g low power wide area networks," in *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*, 2018, pp. 1–9.

[8] A. Yousefpour, G. Ishigaki, and J. P. Jue, "Fog computing: Towards minimizing delay in the internet of things," in *Edge Computing (EDGE), 2017 IEEE International Conference on*. IEEE, 2017, pp. 17–24.

[9] A. Abeshu and N. Chilamkurti, "Deep learning: the frontier for distributed attack detection in fog-to-things computing," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 169–175, 2018.

[10] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[11] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in *Services (SERVICES), 2015 IEEE World Congress on*. IEEE, 2015, pp. 21–28.

[12] H. Habibzadeh, T. Soyata, B. Kantarci, A. Boukerche, and C. Kaptan, "Sensing, communication and security planes: A new challenge for a smart city system design r," *Computer Networks*, vol. 144, pp. 163–200, 2018.

[13] N. Moustafa and J. Slay, "Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set)," in *Military Communications and Information Systems Conference (MilCIS), 2015*. IEEE, 2015, pp. 1–6.

[14] N. Koroniotis, N. Moustafa, E. Sitnikova, and J. Slay, "Towards developing network forensic mechanism for botnet activities in the iot based on machine learning techniques," in *Mobile Networks and Management: 9th International Conference, MONAMI 2017, Melbourne, Australia, December 13-15, 2017, Proceedings*, vol. 235. Springer, 2018, pp. 30–44.

[15] M. Nobakht, V. Sivaraman, and R. Boreli, "A host-based intrusion detection and mitigation framework for smart home iot using openflow," in *Availability, Reliability and Security (ARES), 2016 11th International Conference on*. IEEE, 2016, pp. 147–156.

[16] D. H. Summerville, K. M. Zach, and Y. Chen, "Ultra-lightweight deep packet anomaly detection for internet of things devices," in *Computing and Communications Conference (IPCCC), 2015 IEEE 34th International Performance*. IEEE, 2015, pp. 1–8.

[17] S. Raza, L. Wallgren, and T. Voigt, "Svelte: Real-time intrusion detection in the internet of things," *Ad hoc networks*, vol. 11, no. 8, pp. 2661–2674, 2013.

[18] S. Garg, K. Kaur, N. Kumar, S. Batra, and M. S. Obaidat, "Hyclass: Hybrid classification model for anomaly detection in cloud environment," in *2018 IEEE International Conference on Communications (ICC)*. IEEE, 2018, pp. 1–7.

[19] M. Tavallaee, N. Stakhanova, and A. A. Ghorbani, "Toward credible evaluation of anomaly-based intrusion-detection methods," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 40, no. 5, pp. 516–524, 2010.

[20] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, 2016.

[21] S. Prabavathy, K. Sundarakantham, and S. M. Shalinie, "Design of cognitive fog computing for intrusion detection in internet of things," *Journal of Communications and Networks*, vol. 20, no. 3, pp. 291–298, 2018.

[22] D. Oh, D. Kim, and W. W. Ro, "A malicious pattern detection engine for embedded security systems in the internet of things," *Sensors*, vol. 14, no. 12, pp. 24 188–24 211, 2014.

[23] N. Moustafa and J. Slay, "The evaluation of network anomaly detection systems: Statistical analysis of the unsw-nb15 data set and the comparison with the kdd99 data set," *Information Security Journal: A Global Perspective*, vol. 25, no. 1-3, pp. 18–31, 2016.

[24] M. M. Rathore, A. Paul, A. Ahmad, N. Chilamkurti, W.-H. Hong, and H. Seo, "Real-time secure communication for smart city in high-speed big data environment," *Future Generation Computer Systems*, vol. 83, pp. 638–652, 2018.

[25] J. Zhang, M. Zulkernine, and A. Haque, "Random-forests-based network intrusion detection systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 38, no. 5, pp. 649–659, 2008.

[26] K. Angrishi, "Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets," *arXiv preprint arXiv:1702.03681*, 2017.

[27] A. Alqazzaz, I. Alrashdi, E. Aloufi, M. Zohdy, and H. Ming, "Secsps: A secure and privacy-preserving framework for smart parking systems," *Journal of Information Security*, vol. 9, no. 04, pp. 299–314, 2018.

[28] B. Schneierl. Security econmics of the internet of things,. [Online]. Available: https://bit.ly/2OBuxBE

[29] S. Learn. scikit-learn machine learning in python. [Online]. Available: https://scikit-learn.org/stable/

[30] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in *Wireless Networks and Mobile Communications (WINCOM), 2016 International Conference on*. IEEE, 2016, pp. 258–263.