

Combining Statistical and Machine Learning Techniques in IoT Anomaly Detection for Smart Homes

Georgios Spanos, Konstantinos M. Giannoutakis, Konstantinos Votis, Dimitrios Tzovaras

Information Technologies Institute (ITI)

Center for Research & Technology Hellas (CERTH)

6th km Harilaou - Thermi, 57001

Thessaloniki, Greece

{gspanos,kgiannou,kvotis,Dimitrios.Tzovaras}@iti.gr

Abstract—In this paper, a security solution is proposed for IoT smart homes based on constructing behavioral device templates. These templates are being calculated by combining statistical and machine learning techniques according to their network behavior, captured within a smart home. The statistical metrics generated are being processed in order to produce the appropriate features, which are then used for constructing clusters of devices. The main idea relies on the fact that during an abnormal event, the device will be moved away from the center of the cluster, generating an alert that can be further used for proposing mitigation actions.

The methodology followed in the proposed approach is given in detail, while validation is performed on a real smart home dataset. This work is part of a transparent cyber security framework developed under EU H2020 Project GHOST.

Index Terms—Internet of Things, Smart Home, Anomaly Detection, Information Security, Machine Learning, Statistics.

I. INTRODUCTION

During the last decade, the Internet of Things (IoT) paradigm attracted a great attention from research and commercial communities. As these communities grow, the need for shielding IoT infrastructures from traditional and specialized cyber attacks becomes of great importance. This is being reinforced by several projections that have been performed and indicate that a massive number of such devices will be part of computing networks in the following years.

The high heterogeneity of devices and supported network protocols (such as Ethernet, Bluetooth, Zigbee, rf869 etc.) does not allow the direct application of traditional cyber security solutions, but specialized security software should be developed and/or adjusted. Taking also into consideration the specific communication patterns of some devices/protocols

(e.g. the low communication frequency of a door sensor), the need for specialized solutions is indispensable.

This paper is focused on the detection of abnormalities of IoT devices, in terms of their network traffic within smart homes. Usually, smart homes consist of a gateway responsible for collecting and aggregating sensors data and the sensors/IoT devices, while network sniffing tools are used for collecting the network packages being exchanged between these. The proposed work collects these traffic data trying to classify the devices into behavioral templates/profiles according to a set of predefined features. The generated templates can be then used for detecting anomalies occurred, when a device deviates from its normal behavior, i.e. the distance from the template grows.

This work is part of a transparent cyber security framework developed under EU H2020 Project GHOST, [1], and is expected to provide support on vulnerability assessment procedures.

The rest of the paper is organised as follows: Section II discusses related work on anomaly detection focusing on IoT related environments with machine learning techniques. Section III presents the methodology and procedures developed, while in Section IV evaluation is being performed using a generated dataset on a real smart home infrastructure with two types of attacks. Finally, Section V concludes the paper and provides possible future directions.

II. RELATED WORK

The problem of *Anomaly Detection* has been studied extensively in the literature of many diverse research fields and disciplines the last decades. A representative survey that reflects the multidisciplinary dimension of the problem and presents the different existing techniques, which have been applied so far, can be found on [2]. According to this survey, the following techniques: *Classification*, *Clustering*, *Nearest Neighbor*, *Statistical*, *Information Theoretic* and *Spectral*, have been applied to the domains: *Cyber-Intrusion Detection*, *Fraud Detection*, *Medical Anomaly Detection*, *Industrial Damage Detection*, *Image Processing*, *Textual Anomaly Detection* and *Sensor Networks*.

978-1-7281-1016-5/19/\$31.00 ©2019 IEEE

This work is partially funded by the European Union's Horizon 2020 Research and Innovation Programme through GHOST project (<https://www.ghost-iot.eu/>) under Grant Agreement No. 740923.

Please cite as: Spanos, G., Giannoutakis, K. M., Votis, K., & Tzovaras, D. (2019, September). Combining Statistical and Machine Learning Techniques in IoT Anomaly Detection for Smart Homes. In 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) (pp. 1-6). IEEE.

<https://ieeexplore.ieee.org/abstract/document/8858490>

Regarding the domain of the Fraud Detection, the authors in [3] applied the *Peer Group Analysis* [4] and the *Break Point Analysis* [3] in order to detect possible fraudulent transactions that can occur by using credit cards. Moreover, in [5], a new approach, which is based on the *nearest neighbor* technique, has been introduced in order to detect anomalies in time series that depict electrocardiograms. Furthermore, the authors in [6] proposed a method based on *Kernel Principal Components Analysis* (PCA) [7] to detect anomalies in spacecrafts. They used past normal telemetry data in order to create behavioral model of the system. Finally, in the *Image Processing* field, a *neural network* based framework is proposed [8], in order to detect novel events. According to this approach, if the neural network classifier is not confident about its prediction, then the image could be characterized as novel.

As mentioned before, one of the application domains of the anomaly detection problem is the **Network Security**, which is also, the research field of the present study. A recent survey summarizes the research that has been conducted in this field [9] and reports that in the existing literature the following four techniques have been performed to detect anomalies: *Classification*, *Statistical*, *Clustering* and *Information Theory*. The output of these anomaly detection techniques can be either a label (normal or abnormal behavior) or a score (e.g. a continuous value ranges from 0 to 1) that reflects the magnitude of the abnormality.

The authors in [10] used the *x-means* clustering algorithm, which is a variant of the well-known *k-means* algorithm and suitable for collective anomaly detection. The authors stated that successfully identified *Denial of Service* (DoS) attacks in the network traffic. Furthermore, the authors in [11] combined four well-established detection approaches: *time-based detection*, *Neyman-Pearson detection*, *Bayesian Network decision approach* and *early detection*, to detect outages on telecommunication network. Finally, a *non-linear correlation* approach based on *mutual information* has been proposed by the authors in [12] in order to reduce the false positive alarms in the intrusion detection systems.

In the IoT research field, a recent study [13] used a flow-based security solution to detect attacks in IoT devices. Moreover, the authors in [14] used the network traffic of IoT devices to detect anomalies. More specifically, they used statistical techniques, such as the *Euclidean Distance* similarity metric and the computation of the upper and lower limits of the normal behavior from the *standard deviation* metric. Finally, several studies [15]–[18] in the IoT research field have as main research goal the identification of the IoT devices, which is usually, a prerequisite step in order to distinguish the authorized devices from the unauthorized devices and possibly, to detect abnormal behavior. For this reason, different single or ensemble *classification* algorithms were conducted in the corresponding studies.

It is obvious from the aforementioned that the research activity in the field of IoT is emerging and the field needs a lot of attention. Moreover, to the best of our knowledge there is not a research study until now that combines statistical and

machine learning techniques such as: *Descriptive Statistics*, *PCA*, *Clustering* and *Classification* in order to detect anomalies in IoT devices.

III. METHODOLOGY

As already mentioned, the proposed methodology combines well-established statistical and machine learning methodologies to network traffic data in order to detect abnormal behavior of the IoT devices. This anomaly detection framework consists of two phases: the *Training Phase* and the *Running Phase*. The *Training Phase* is executed periodically and updates the models, whereas the *Running Phase* runs continuously using the models of the *Training Phase*.

Fig. 1 depicts the steps of the *Training Phase*. The first step of the methodology is the extraction of the following statistical metrics for each connected to the gateway IoT device: *Min*, *Max*, *Average*, *25%*, *Median*, *75%*, *Standard Deviation*, *Interquartile Range*, from the network traffic data, which is the input of the methodology. The data from the network traffic are related to the: *Size of the Packets*, *Time Interval between Packets/Flows*, *Number of Packets*, *Duration of the Communications* and *Number of Different Communications*. The extraction of the statistical features that were described above is inspired by the work in [19].

After the feature extraction, the next step before the conduction of the sophisticated statistical and machine learning techniques, is the *Standardization* of the features. The usefulness of the *Standardization* in different scale variables is incontrovertible, as reflected also in the literature [20]. Next, *PCA* follows in order to create uncorrelated variables from the original dataset. Apart from the property of *PCA* to create uncorrelated variables, which are called principal components, *PCA* is also, a suitable method to reduce the initial number of features and keep only the most important principal components. In the proposed methodology, the Jolliffe modification [21] of the Gutman-Kaiser criterion was selected to keep the most important principal components. The reason to select this modification is that improves -regarding the reliability- the Gutman-Kaiser criterion, which is a very popular criterion to the statistical community [22].

The next step of the methodology is the *clustering* of the IoT devices according to their network normal behavior and this is the main novelty of the present study. This consideration is based on the basic principles of the *Peer Group Analysis* [4]. The *Density Based Spatial Clustering* (DBSCAN) [23] was selected for the clustering procedure, due to its simplicity, which is reflected by the fact that there is no need to predetermine the number of clusters and due to its superiority over other clustering algorithms, regarding the performance [24]. Finally, using the clusters as labels, an ensemble classifier is trained, having as independent variables the previously calculated values of the principal components and as dependent variable the label-cluster. The specific ensemble classifier combines the following well-established classifiers -which are also widely used in the machine learning community-: *Random Forest*, *Naïve Bayes*, *Support Vector Machine* and

Decision Tree. The final estimation is derived from the soft voting [25] of the above classifiers and more precisely, from the probability scores of each classifier. The selection of an ensemble classifier instead of a single classifier, follows the guidelines of the recent literature in machine learning [26]. Similarly, the soft voting was selected for the final estimation instead of the hard/majority voting, since when the classifiers have the ability to produce a probability score for each class as output, this is the appropriate strategy in the machine learning literature [25]. Finally, the reasoning behind the selection to combine the classification with the clustering algorithms, is explained extensively at the description of the *Running Phase*.

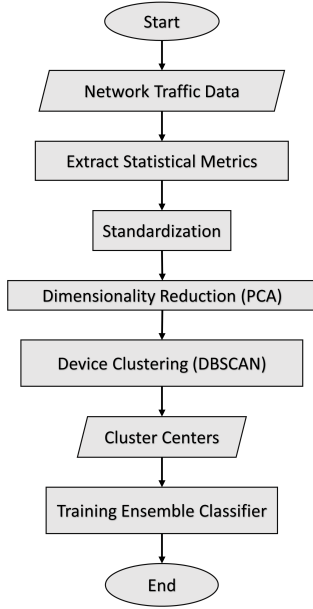


Fig. 1. Training Phase of the Proposed Methodology

The steps of the *Running Phase* are displayed in Fig. 2. It is obvious from the *Running Phase* flowchart that the steps until the check for new devices are identical to the *Training Phase* flowchart. Hence, the algorithm during the *Running Phase*, uses as input the live network data and from these data extracts the statistical features. The difference with the *Training Phase* is that during the *Running Phase*, the next steps of the: *Standardization* and *PCA* are conducted using the corresponding fitting parameters of the *Training Phase*.

Moreover, when new devices are connected to the IoT Ecosystem, the ensemble classifier tries to classify them into one of the existing classes that represent the corresponding clusters. If the classifier is not confident (e.g. the probability score is below a specific threshold) about the class/cluster that the new device belongs to, then a new cluster is created to include this new IoT device. The proposed approach that combines the clustering with the classification is based on the fact that during the *Running Phase*, a) the new devices should be grouped quickly without the need of a time consuming procedure such as the clustering and b) the cluster templates of the *Training Phase* should remain the same.

The last step of the methodology is the computation of the well-known Euclidean distance metric, between each IoT device and the previously calculated center of the cluster in which the IoT device is a member. The Euclidean distance formula is displayed below:

$$D(X, Y) = \sqrt{\sum_{i=1}^n (X_i - Y_i)^2} \quad (1)$$

where X , is the feature vector of the cluster center, Y , is the corresponding vector of the IoT device and n , the number of features. From the Euclidean distance, a threat score for each IoT device is produced as follows: if the distance of an IoT device from the center of the cluster that belongs to, is lower than a threshold, then a safe score of 1 is produced, otherwise the threat score is computed from the following fraction:

$$threat\ score = \frac{threshold}{Euclidean\ Distance} \quad (2)$$

It is obvious from the above equation that as the threat score is getting closer to 0, the risk is getting higher, since the Euclidean Distance of the IoT device from the cluster center (e.g. the distance from its normal behavior) is getting larger.

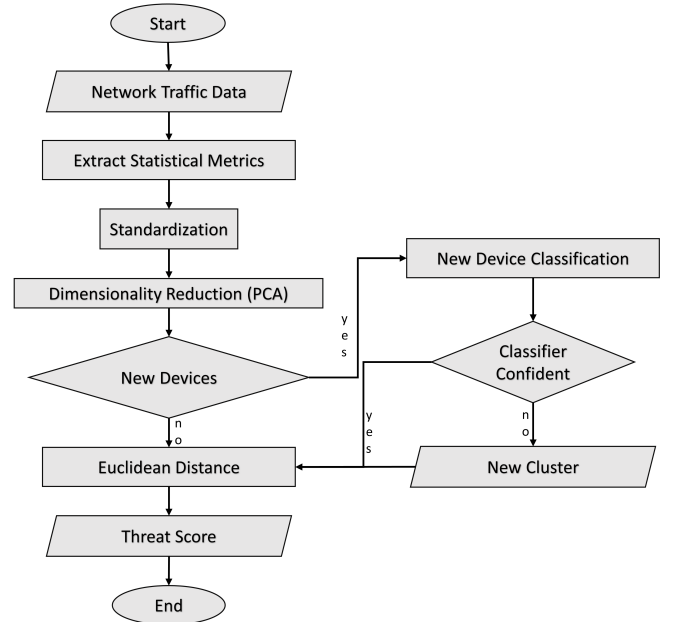


Fig. 2. Running Phase of the Proposed Methodology

The algorithm, which was described in this Section, was implemented in Python¹, which is one of the most popular programming language with strong community of developers and suitable for machine learning applications. More specifically, for the statistical and machine learning part of the algorithm the well-established package Scikit-learn [27] of Python was used.

¹<https://www.python.org/>

A. Validation

To validate the proposed methodology regarding its ability to detect anomalies, two different types of attack to the IoT Devices will be emulated:

- *Physical Damage*, which reflects an attack such as the steal of an IoT device or its destruction from a person that has physical access to this device, having as a result the stop of the communication between this device and the gateway.
- *Mechanical Exhaustion*, which represents an attack to an IoT device, where an attacker has as previously, physical access to the device and triggers it repeatedly, having as target to exhaust mechanically the device. This type of attack would lead to an increased abnormal behavior of the IoT device regarding its network traffic.

IV. RESULTS

In this Section, the results of the experiments are presented. The dataset is derived from a test bed of the GHOST project and consists of 5 IoT devices that support the protocol Z-Wave², which is one of the most popular protocols used in the smart homes. These devices are shown in Table I.

TABLE I
IoT DEVICES - DESCRIPTION

Device No	Device Description
1	PST02-A 4 in 1 Multisensor
2	ZW100 Multisensor 6
3	ZDZ2102 Door/Window Sensor
4	AT02 1-B 2 in 1 Sensor
5	AN180-2 Miniplug

During the *Training Phase*, each IoT Device formed a different cluster (total 5 clusters), according to their transformed values (after the PCA transformation) on the Principal Components (PC) and subsequently, these values correspond to the cluster centers. The PC values of each IoT Device are shown in Table II. Moreover, Fig 3 displays the five IoT devices according to their PC values in 4d-representation. The first three dimensions corresponds to the well-known Euclidean space, while the fourth dimension is represented in the graph as the size of each sphere.

TABLE II
PRINCIPAL COMPONENTS VALUES

Device No	PC 1	PC 2	PC 3	PC 4
1	-0.06	0.26	1.20	1.3
2	-0.5	-1.16	-1.11	0.62
3	0.12	-0.89	0.89	-1.26
4	-1.13	1.21	-0.36	-0.58
5	1.57	0.58	-0.63	-0.08

To emulate the first attack (*Physical Damage*) all the devices stopped to communicate with the gateway for some time and this emulation reflects perfectly the network behavior, in the

case that someone had stolen the devices. At this point, it is important to mention that one of the devices (Device No. 5), had not network traffic during the *Training Phase*. The results of this experiment are displayed in Table III and Fig. 4. It is obvious from the results that all the devices (apart from the idle device during the *Training Phase*) fell below the safe score of 1 (threat score is 0.88), and graphically this behavior is depicted by the movement of the four devices (yellow, red, cyan and green spheres) to the fifth device (orange sphere) which was idle at the *Training Phase*.

TABLE III
EXPERIMENTATION RESULTS

Device No	Threat Score	
	<i>Physical Damage</i>	<i>Mechanical Exhaustion</i>
1	0.88	0.15
2	0.88	0.36
3	0.88	0.52
4	0.88	0.30
5	1	0.13

Similarly, to emulate the second attack (*Mechanical Exhaustion*), all the devices triggered repeatedly for some time as exactly in the case that someone would like to exhaust mechanically the IoT devices. The results are shown in Table III and Fig. 5 and it is clear that for this type of attack, the threat scores for all the IoT devices (from 0.13 to 0.52) along with the large movements in the graph reflect the existence of an anomaly in the network behavior.

V. CONCLUSIONS

Statistical and Machine Learning techniques were combined in this research study in order to detect anomalies in the network behavior of IoT devices. Preliminary experiments were conducted in a dataset that consists of five IoT devices that support the Z-Wave protocol in order to detect two different types of attacks. The results of the experiments as presented in the previous Section are encouraging.

The proposed methodology managed to detect both the *Physical Damage* and the *Mechanical Exhaustion* attacks, since the corresponding threat scores for both attacks were below the safe score. An important observation that needs attention in the future is the difference in the threat scores and in the corresponding graphical representations for the two different types of attacks, since it seems that the detection of the *Mechanical Exhaustion* is easier than the detection of the *Physical Damage*. A possible interpretation, regarding the different behavior of the methodology that depends on the type of attack (*Physical Damage* or *Mechanical Exhaustion*), could be that the normal network behavior of these type of devices (smart home devices) is relatively rare and hence, the *Physical Damage* attack is more difficult to detect it.

As future work, more experiments will be performed in order to validate that the proposed methodology is able to detect different types of attacks, including the traditional network attacks (Denial of Service and Distributed Denial of Service) and the common software attacks that exploit the

²<https://www.z-wave.com/>

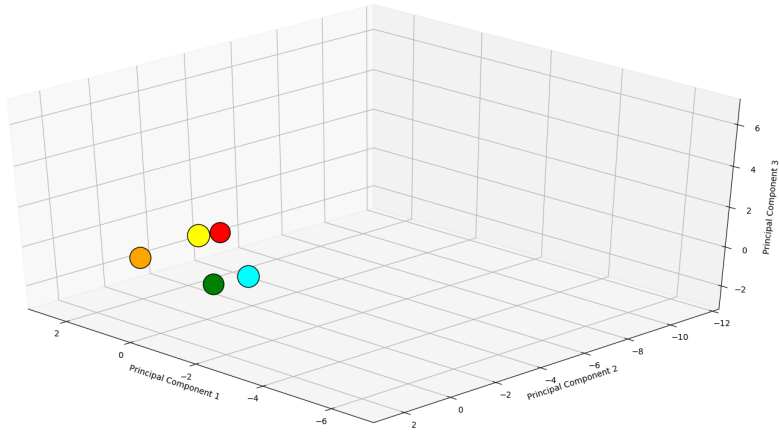


Fig. 3. 4D Representation of the IoT Devices - Training

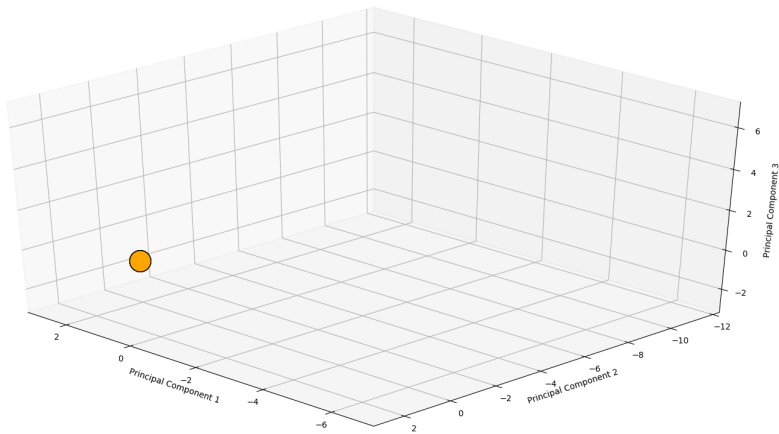


Fig. 4. 4D Representation of the IoT Devices - Physical Damage

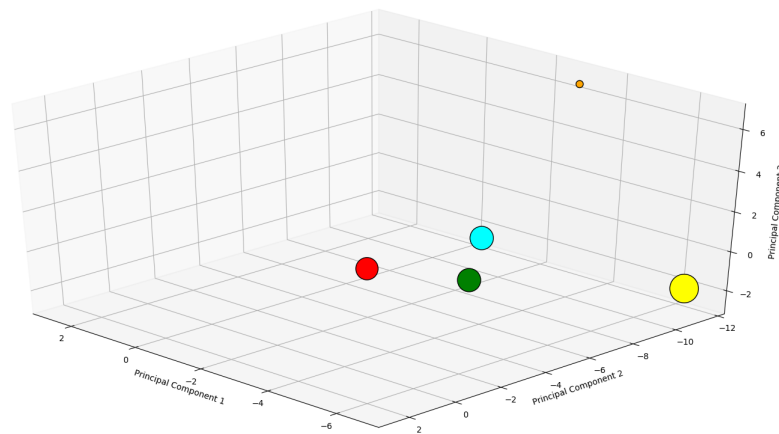


Fig. 5. 4D Representation of the IoT Devices - Mechanical Exhaustion

software vulnerabilities. Moreover, in the future experiments that will take place in real smart homes, the focus will be on the IoT device clustering and for this reason the number of the IoT devices will be much more larger (including different network protocols) in order to have reliable clusters that better reflect the network behavior of the IoT devices.

A crucial point of the proposed methodology is the determination of the threshold that distinguishes the safe normal behavior from the abnormal behavior. If a very low threshold selected then it is possible to have frequently false alarms. On the other hand, if a high threshold selected then attacks that do not impact significantly the network behavior will be undetectable. For this reason, this threshold will be the main focus on the future experimentation.

ACKNOWLEDGMENT

This work is partially funded by the European Union's Horizon 2020 Research and Innovation Programme through GHOST project (<https://www.ghost-iot.eu/>) under Grant Agreement No. 740923. The authors would like to acknowledge Bela Genge from Kalos Information Systems AS, for providing the smart home datasets.

REFERENCES

- [1] A. Collen, N. A. Nijdam, J. Augusto-Gonzalez, S. K. Katsikas, K. M. Giannoutakis, G. Spathoulas, E. Gelenbe, K. Votis, D. Tzovaras, N. Ghavami, M. Volkamer, P. Haller, A. Sánchez, and M. Dimas, "Ghost - safe-guarding home iot environments with personalised real-time risk control," in *Security in Computer and Information Sciences*, E. Gelenbe, P. Campegiani, T. Czachórski, S. K. Katsikas, I. Komnios, L. Romano, and D. Tzovaras, Eds. Cham: Springer International Publishing, 2018, pp. 68–78.
- [2] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM computing surveys (CSUR)*, vol. 41, no. 3, p. 15, 2009.
- [3] R. J. Bolton, D. J. Hand *et al.*, "Unsupervised profiling methods for fraud detection," in *Proc. Credit Scoring and Credit Control VII*. Citeseer, 2001.
- [4] R. J. Bolton and D. J. Hand, "Peer group analysis—local anomaly detection in longitudinal data," Technical Report, Department of Mathematics, Imperial College, London, Tech. Rep., 2001.
- [5] J. Lin, E. Keogh, A. Fu, and H. Van Herle, "Approximations to magic: Finding unusual medical time series," in *null*. IEEE, 2005, pp. 329–334.
- [6] R. Fujimaki, T. Yairi, and K. Machida, "An approach to spacecraft anomaly detection problem using kernel feature space," in *Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining*. ACM, 2005, pp. 401–410.
- [7] B. Schölkopf, A. Smola, and K.-R. Müller, "Nonlinear component analysis as a kernel eigenvalue problem," *Neural computation*, vol. 10, no. 5, pp. 1299–1319, 1998.
- [8] S. Singh and M. Markou, "An approach to novelty detection applied to the classification of image regions," *IEEE Transactions on Knowledge and Data Engineering*, vol. 16, no. 4, pp. 396–407, 2004.
- [9] 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.
- [10] M. Ahmed and A. N. Mahmood, "Network traffic analysis based on collective anomaly detection," in *2014 9th IEEE Conference on Industrial Electronics and Applications*. IEEE, 2014, pp. 1141–1146.
- [11] Ž. Deljac, M. Randić, and G. Krčelić, "Early detection of network element outages based on customer trouble calls," *Decision Support Systems*, vol. 73, pp. 57–73, 2015.
- [12] M. A. Ambusaidi, Z. Tan, X. He, P. Nanda, L. F. Lu, and A. Jamdagni, "Intrusion detection method based on nonlinear correlation measure," *International journal of internet protocol technology*, 2014.
- [13] A. Sivanathan, D. Sherratt, H. H. Gharakheili, V. Sivaraman, and A. Vishwanath, "Low-cost flow-based security solutions for smart-home iot devices," in *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. IEEE, 2016, pp. 1–6.
- [14] J. Pacheco and S. Hariri, "Anomaly behavior analysis for iot sensors," *Transactions on Emerging Telecommunications Technologies*, vol. 29, no. 4, p. e3188, 2018.
- [15] Y. Meidan, M. Bohadana, A. Shabtai, J. D. Guarnizo, M. Ochoa, N. O. Tippenhauer, and Y. Elovici, "Profiliot: a machine learning approach for iot device identification based on network traffic analysis," in *Proceedings of the symposium on applied computing*. ACM, 2017, pp. 506–509.
- [16] Y. Meidan, M. Bohadana, A. Shabtai, M. Ochoa, N. O. Tippenhauer, J. D. Guarnizo, and Y. Elovici, "Detection of unauthorized iot devices using machine learning techniques," *arXiv preprint arXiv:1709.04647*, 2017.
- [17] A. Sivanathan, D. Sherratt, H. H. Gharakheili, A. Radford, C. Wijenayake, A. Vishwanath, and V. Sivaraman, "Characterizing and classifying iot traffic in smart cities and campuses," in *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2017, pp. 559–564.
- [18] A. Sivanathan, H. H. Gharakheili, F. Loi, A. Radford, C. Wijenayake, A. Vishwanath, and V. Sivaraman, "Classifying iot devices in smart environments using network traffic characteristics," *IEEE Transactions on Mobile Computing*, 2018.
- [19] N. Aluthge, "Iot device fingerprinting with sequence-based features," Master's thesis, University of Helsinki, Department of Computer Science, helda.helsinki.fi, 12 2017.
- [20] S. Suthaharan, "Big data analytics," in *Machine Learning Models and Algorithms for Big Data Classification*. Springer, 2016, pp. 31–75.
- [21] I. T. Jolliffe, *Principal component analysis*, 2nd ed. New York, NY: Springer, 2002.
- [22] I. Jolliffe, *Principal component analysis*. Springer, 2011.
- [23] H.-P. Kriegel, P. Kröger, J. Sander, and A. Zimek, "Density-based clustering," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 1, no. 3, pp. 231–240, 2011.
- [24] J. M. Dudik, A. Kurosu, J. L. Coyle, and E. Sejdić, "A comparative analysis of dbscan, k-means, and quadratic variation algorithms for automatic identification of swallows from swallowing accelerometry signals," *Computers in biology and medicine*, vol. 59, pp. 10–18, 2015.
- [25] A. Géron, *Hands-on machine learning with Scikit-Learn and TensorFlow: concepts, tools, and techniques to build intelligent systems*. O'Reilly Media, Inc., 2017.
- [26] L. Rokach, "Ensemble-based classifiers," *Artificial Intelligence Review*, vol. 33, no. 1-2, pp. 1–39, 2010.
- [27] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, "Scikit-learn: Machine learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.