Machine Learning for the Internet of Things Security: A Systematic Review

Darko Andročec and Neven Vrček
Faculty of Organization and Informatics, University of Zagreb, Pavlinska 2, Varaždin, Croatia

Keywords: Machine Learning, Internet of Things, IoT, Security, Systematic Review.

Abstract: Internet of things (IoT) is nowadays one of the fastest growing technologies for both private and business purposes. Due to a big number of IoT devices and their rapid introduction to the market, security of things and their services is often not at the expected level. Recently, machine learning algorithms, techniques, and methods are used in research papers to enhance IoT security. In this paper, we systematically review the state-of-the art to classify the research on machine learning for the IoT security. We analysed the primary studies, identify types of studies and publication fora. Next, we have extracted all machine learning algorithms and techniques described in primary studies, and identified the most used ones to tackle IoT security issues. We classify the research into three main categories (intrusion detection, authentication and other) and describe the primary studies in detail to analyse existing relevant works and propose topics for future research.

1 INTRODUCTION

Market of smart things is growing constantly. Both established hardware companies and start-ups introduce their new devices (things – sensors, actuators, and microcontrollers), Internet of Things (IoT) software, IoT services and platforms. Their main motivation is to release their innovative IoT products and services as fast as possible, to gain the competitive advantage on the market. For this reason, many IoT products and services are not designed with security in mind. Nowadays, we are witnessing botnets and other types of malicious software that exploit the various vulnerabilities of IoT devices and services. Due to high number of IoT devices, this fact can represent a huge security risk, e.g. malicious software on devices can initiate a massive distributed denial of service (DDoS) attack against the target web site or information system. For this reason, security is a very important research and professional topic in the Internet of Things area.

Furthermore, sensors generate enourmous quantity of data. The dominant method nowadays to deal with Big Data is a machine learning. The machine learning algorithm is given the goal(s) and then it learns from the data which factors are important in achieving that goal.

The main contribution of this paper is a systematic review of existing literature on machine learning for the IoT security. Such comprehensive review does not exist in the current literature. In 2015, the data mining literature for the Internet of Things was reviewed by Chen et al. (2015), but their focus was not on machine learning and IoT security. The paper written by Mahdavinejad et al. (2017) assesses the different machine learning methods that deal with the challenges in IoT data by considering smart cities as the main use case. IoT security was not tackled in the before mentioned paper. The primary aim of our research is to provide an overview of machine learning techniques and methods used to improve IoT security, to classify the relevant state-of-the art research, and to identify possible future research ideas and challenges.

For remainder, this paper is organized as follows: Section 2 describes the research method used for our systematic literature review. The next section lists the results and provides a discussion about obtained results of the systematic review. Our conclusions are provided in the final section.

2 RESEARCH METHOD

Our research has been carried according to the systematic literature review (SLR) methodology

Andročec, D. and Vrček, N.
Machine Learning for the Internet of Things Security: A Systematic Review.
DOI: 10.5220/0006841205630570
In *Proceedings of the 13th International Conference on Software Technologies (ICSOFT 2018)*, pages 563-570
ISBN: 978-989-758-320-9

(Kitchenham and Charters, 2007). Systematic reviews must be undertaken in accordance with a predefined search strategy, and the main phases of SLR are (Kitchenham and Charters, 2007): Planning (identification of the need for a review, specification of the research questions, development of a review protocol); Conducting (identification of research, selection of primary research study quality assessment, data extraction and monitoring, data synthesis); and Reporting (specification of dissemination mechanisms, formatting the main report, evaluation of the report). These main steps of the SLR protocol are explained in the following subsections.

2.1 Planning the Review

We developed a review protocol in the planning phase of the SLR procedure. We have described and explained the needs for a systematic review on machine learning for the IoT security in the Introduction. Next, we have defined the following research questions:

RQ1: What are the most used machine learning algorithms/techniques/methods for IoT security papers?

RQ2: How can we classify machine learning for IoT security papers?

Based on the stated research questions and objectives of our study, we have defined the review protocol. We have also performed a pilot study of the systematic review of ten sample studies from IEEE Xplore Digital Library to refine the research questions and to define the inclusion and exclusion criteria. We focused on the following electronic scientific databases: IEEE Xplore, Web of Science Core Collection, and Scopus. The search term was defined as "security machine learning Internet of things".

We did not limit our search to specific time period, because our pilot search showed that all the works that we found are relatively new. Next, we defined the following inclusion criteria: the paper must investigate about machine learning for IoT security, only research (scientific) papers were included that were published as a conference paper, journal paper or scientific book chapter, and the paper must be written in English. We excluded papers that were not related to our stated research questions, papers that not discuss all three areas (security, Internet of things, and machine learning), duplicate studies, non-English papers, *Powerpoint* presentations, preliminary studies, posters, and proof-of-concept papers.

2.2 Conducting the Review

The second main phase of the systematic review protocol defined by (Kitchenham and Charters, 2007) is conducting the review. We have performed the search by using the search procedure defined in the previous subsection on 27th February 2018. The mentioned search was performed on the three electronic scientific databases (IEEE Xplore Digital Library, Web of Science Core Collection, and Scopus), and studies were excluded based on exclusion criteria. Next, studies were excluded based on their titles and abstracts. The papers that remain after these two initial filters, were fully read. To make this process quicker, we have used a free reference management system *Zotero*.

During our first search, a total of 284 papers were identified. After filtering the publications list (using defined inclusion/exclusion criteria) by reading their titles and abstracts, full text reading of the articles that had not been excluded was performed to ensure that the content is related to our research questions. Finally, 26 studies (Table 1) were identified as primary studies, and their data relevant to our research questions were extracted to Excel spreadsheet. Papers are given identifiers P1-P26 (Table1).

Table 1: The Selected Primary Studies.

ID	Reference	Title
P1	(Nobakht et al., 2016)	A Host-Based Intrusion Detection and Mitigation Framework for Smart Home IoT Using OpenFlow
P2	(Wang et al., 2017)	Current Mirror Array: A Novel Circuit Topology for Combining Physical Unclonable Function and Machine Learning
P3	(Aminanto et al., 2018)	Deep Abstraction and Weighted Feature Selection for Wi-Fi Impersonation Detection
P4	(Abeshu and Chilamkurti, 2018)	Deep Learning: The Frontier for Distributed Attack Detection in Fog-to-Things Computing
P5	(Indre and Lemnaru, 2016)	Detection and prevention system against cyber attacks and botnet malware for information systems and Internet of Things
P6	(Bhunia and Gurusamy, 2017)	Dynamic attack detection and mitigation in IoT using SDN
P7	(Liu et al., 2018)	EPIC: A Differential Privacy Framework to Defend Smart Homes Against Internet Traffic Analysis
P8	(Baldini et al., 2017b)	Imaging time series for internet of things radio frequency fingerprinting

Table 1: The Selected Primary Studies (cont.).

ID	Reference	Title
P9	(Zissis, 2017)	Intelligent security on the edge of the cloud
P10	(Perez et al., 2017)	Intrusion detection in computer networks using hybrid machine learning techniques
P11	(Gao and Thamilarasu, 2017)	Machine-Learning Classifiers for Security in Connected Medical Devices
P12	(Ahmed et al., 2017)	Mitigating DNS query-based DDoS attacks with machine learning on software-defined networking
P13	(Baldini et al., 2017a)	Physical layer authentication of Internet of Things wireless devices through permutation and dispersion entropy
P14	(Razeghi et al., 2017)	Privacy preserving identification using sparse approximation with ambiguization
P15	(Lee et al., 2017)	ProFiOt: Abnormal Behavior Profiling (ABP) of IoT devices based on a machine learning approach
P16	(Cho et al., 2017)	Security Assessment of Code Obfuscation Based on Dynamic Monitoring in Android Things
P17	(Roux et al., 2017)	Toward an Intrusion Detection Approach for IoT Based on Radio Communications Profiling
P18	(Yeh et al., 2016)	Transparent authentication scheme with adaptive biometrie features for IoT networks
P19	(Canedo and Skjellum, 2016)	Using machine learning to secure IoT systems
P20	(Aminanto et al., 2017)	Wi-Fi intrusion detection using weighted-feature selection for neural networks classifier
P21	(Wu et al., 2017)	Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods
P22	(Diro and Chilamkurti, 2018)	Distributed attack detection scheme using deep learning approach for Internet of Things
P23	(Gebrie and Abie, 2017)	Risk-based adaptive authentication for internet of things in smart home eHealth
P24	(Ali et al., 2018)	Trust in IoT: dynamic remote attestation through efficient behavior capture
P25	(Outchakoucht et al., 2017)	Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things
P26	(Domb et al., 2017)	Lightweight adaptive Random-Forest for IoT rule generation and execution

In the end, we extracted data from the selected primary studies and did a synthesis and analysis. The results of the SLR (Reporting phase) are shown in the next section.

3 RESULTS AND DISCUSSION

3.1 Used Machine Learning Algorithms

All of the works is actually very recent. We didn't limit our search to the specific period, and the results have shown that selected papers are from 2016, 2017, and 2018. The number of papers significantly increased in 2017. There is decrease in the number of papers from 2018, but this is a result of our search date of the systematic literature review procedure (February 2018).

Regarding publication types, most of the primary studies are conference papers (sixteen), followed by 10 journal papers. The publisher of the most papers is IEEE (20 primary studies), followed by Springer (2 papers) and Elsevier (2 papers). . All the papers from 2016 were conference papers. The next year, 5 of 17 published papers were journal papers. All existing papers from 2018 are journal papers. This shows that the research on machine learning for IoT security is more mature and more journals are accepting these types of papers. The primary studies are written by authors with affiliations from twenty countries.

During reading the full-text of the primary studies, we extracted all machine learning algorithms and techniques described in papers and used for IoT security. Some papers used more than one technique. The mentioned data is listed in Table 2.

The most mentioned machine learning algorithms or techniques in the primary studies are: Support Vector Machine (9 papers), Artificial Neural Network (5 papers), Naïve Bayes (4 papers), Decision Tree (4 papers), kNN (3 papers), k-Mean (3 papers), Random forest (3 papers), and Deep Learning (2 papers). All other algorithms and techniques were used only in one paper. These results show that Support Vector Machine (SVM) is most used machine learning method for IoT security. This is not surprise, because SVM is one of the state-of-art methods for machine learning and data mining (Wang, 2005). This method is used in the primary studies both for intrusion detection and for authentication. The support vector machine (SVM) is a supervised learning method that generates input-output mapping functions (either a classification function or a regression function) from a set of labelled training data (Wang, 2005).

Table 2: Used machine learning algorithms.

Paper ID	Used machine learning algorithms / technique / method
P1	Support Vector Machines (SVMs)
P2	Extreme learning machine (ELM)
P3	Support Vector Machine (SVM) and Artificial Neural Network (ANN)
P4	Deep learning (DL)
P5	Used classifiers: Logistic, Linear, SVM, Decision Tree Classifier (Gini, Entropy), Decision Tree Regressor, Naïve Bayes (Gaussian, Multinomial, Bernoulli) ,kNN, K-Mean, Random Forest, Gradient Boosting, SGDC, Passive Aggressive, Mini Batch KMeans, SGDRegressor.
P6	Support Vector Machine (SVM)
P7	- (machine learning is used by attackers)
P8	SVM, KNN, and Decision Trees
P9	One-class Support Vector Machines
P10	Hybrid Machine Learning techniques: Neural Network (NN) and Support Vector Machine (SVM), and K-Means
P11	Decision-Tree Learning
P12	Dirichlet process mixture model (DPMM)
P13	- (statistical methods Permutation Entropy (PE) and the Dispersion Entropy (DE))
P14	Approximate nearest neighbour (ANN) search
P15	k-Means algorithm and support vector machine (SVM)
P16	Naive Bayes
P17	Neural network
P18	Support vector machine with Gaussian radial basis function (SVM-GF)
P19	Artificial neural networks
P20	Artificial Neural Network (ANN), and decision tree
P21	Random forest multi-way classifier, k-nearest neighbours (kNN)
P22	Deep learning
P23	Naive Bayes
P24	Averaged One-Dependence Estimator (AODE), Hidden Naive Bayes (HNB) and Naive-Bayes classifiers
P25	Reinforcement Learning (RL) algorithms
P26	Random forest

Next method of choice is Artificial Neural Network (ANN). Artificial neural networks (ANNs) simulate the way in which the human brain processes information. It is formed from hundreds artificial neurons, connected with coefficients (weights), which are organised in layers (Agatonovic-Kustrin and Beresford, 2000). The various applications of ANNs are classification or pattern recognition, prediction and modelling. In the primary studies, ANN was used for intrusion detection.

Naïve Bayes and Decision Tree are mentioned both in 4 primary studies. These methods were used before in various intrusion detection systems (Amor et al., 2004), so it was expected that they will be also used in IoT security domain. Naive Bayes have several advantages due to their simple structure, but make a strong independence relation assumption that is not always true (Amor et al., 2004). There are also several algorithms developed in order to ensure the construction of decision trees and its use for the classification (Amor et al., 2004).

3.2 Main Themes of Papers

We have identified two main themes of primary studies: intrusion detection and authentication. We also added the category *Other* which includes all papers that cannot be classified into an intrusion detection or an authentication category. The distribution of the papers per category is depicted in Figure 1. The category with the most papers (16) is intrusion detection. We will use this classification to describe papers in more detail in the next subsections.

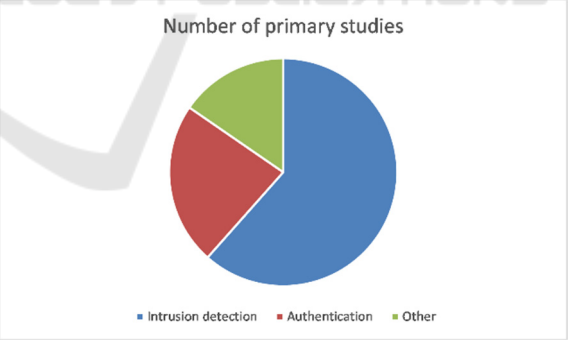

Figure 1: Classification of primary study.

3.2.1 Intrusion Detection

Intrusion detection is the biggest category that consists of 16 papers from our set of primary studies: P1, P3, P4, P5, P6, P9, P10, P11, P12, P15, P17, P19, P20, P21, P22, and P26. In the rest of this subsection, we will describe briefly the main themes of the mentioned papers. Intrusion detection and mitigation framework IoT-IDM (Nobakht et al., 2016) provides a network-level protection for IoT

devices deployed in smart homes. IoT-IDM gives its users the flexibility to employ customized machine learning techniques for detection based on learned signature patterns of known attacks.

Aminanto et al. (2018) propose a modified feature-selection-based method by considering the weights of each feature obtained from lightweight machine-learning models to detect an impersonation attack. Deep model-based attack detection architecture for IoT was proposed for of cyber-attack detection in fog-to-things computing (Abeshu and Chilamkurti, 2018). In the next paper (Indre and Lemnaru, 2016), authors applied concepts of machine learning to select and extract features that can lead to an accurate decision of classification for malware and intrusion attacks.

An SDN-based secure IoT framework called SoftThings is proposed by Bhunia and Gurusamy, (2017) to detect abnormal behaviours and attacks as early as possible. Machine learning is used at the Software-Defined Networking (SDN) controller to monitor and learn the behaviour of IoT devices over time. Machine learning models (specifically Support Vector Machines) are employed on the edge of the cloud, to perform low footprint unsupervised learning and analysis of sensor data for anomaly detection purposes in the study (Zissis, 2017).

The paper written by (Perez et al., 2017) presents the design, implementation and performance analysis of multiple hybrid (combination of supervised and unsupervised learning algorithms) machine learning models for the task of intrusion detection. Gao and Thamilarasu (2017) assess the feasibility of using machine learning models to efficiently determine attacks targeted on medical devices by observing any deviation from its normal behaviour. They tested their method using different machine learning algorithms and provide their comparison analysis. Ahmed et al. (2017) propose a DNS query-based DDoS attack mitigation system using Software-Defined Networking (SDN) to block the network traffic for DDoS attacks. Dirichlet process mixture model (DPMM) was used for clustering traffic flows.

Next, ProFiOt (Lee et al., 2017) is used for Abnormal Behaviour Profiling (ABP) of IoT devices by a wide variety of machine learning algorithms. The proposed ABP was developed and assumed when a malicious attacker modified one aspect of the data from the whole dataset (e.g., just temperature) instead of compromising the whole dataset of specific sensors to mislead the target actuators. An approach to detect potential attacks in smart places (e.g. smart homes) by detecting deviations from legitimate communication behaviour is proposed by Roux et al. (2017). Their solution is based on the profiling and monitoring of the Radio Signal Strength Indication (RSSI) associated to the wireless transmissions of the connected objects. A machine learning neural network algorithm is used to characterize legitimate communications and to identify suspicious scenarios.

Canedo and Skjellum (2016) investigate using Artificial Neural Networks in a gateway to detect anomalies in the data sent from the edge devices. Authors of the next paper (Aminanto et al., 2017) test and validate the feasibility of the selected features using a common neural network to detect known and unknown attacks in Wi-Fi networks. Intrusion detection in cyber manufacturing systems with machine learning methods was shown in the paper (Wu et al., 2017). Two examples were developed with simulation and experiments: 3D printing malicious attack and CNC milling machine malicious attack. Deep learning approach was used by Diro and Chilamkurti (2018) to enable the detection of attacks in social IoT. A lightweight comprehensive IoT rules generation and execution framework is shown in (Domb et al., 2017). It is composed of three components, a machine learning rule discovery, a threat prediction model builder and tools to ensure timely reaction to rules violation and unstandardized and ongoing changes in traffic behaviour. They use Random- Forest (RF) as the machine learning platform for rules discovery and real-time anomaly detection.

3.2.2 Authentication

The next category is authentication and it contains the following 6 papers: P2, P8, P13, P18, P23, and P25. A novel physical unclonable function (PUF) based on current mirror array (CMA) circuits that uses the circuit implementation of the extreme learning machine (ELM) was proposed by Wang et al. (2017). In the paper (Baldini et al., 2017b), the authors have investigated a novel approach to Radio Frequency (RF) fingerprinting where the collected time series are converted to images out of which suitable image-based features are extracted. The extracted features are then used to perform the identification and the verification tasks. The same authors in their second paper (Baldini et al., 2017a) applied RF fingerprinting to IoT devices on the basis of entropy based statistical features called permutation entropy and dispersion entropy.

Next, Yeh et al., (2016) propose an authentication system which applies machine learning techniques to extract user bio-features as

authentication tokens and transparently performs continual or real-time entity verification in the background. Gebrie and Abie (2017) develop a risk-based adaptive authentication mechanism which continuously monitors the channel characteristics variation, analyses a potential risk using naive Bayes machine learning algorithm and performs adaptation of the authentication solution. Furthermore, Ali et al. (2018) have designed and implemented a lightweight Linux kernel security module for IoT devices to monitor multiple applications in the kernel space. Verification of behaviour of applications is performed via machine learning techniques, and design of an architecture for verification of multiple applications on mobile platforms and other smart devices was implemented.

3.2.3 Other Papers

Other papers include paper on privacy of IoT network traffic (P7), privacy preserving identification (P14), code obfuscation in Android things (P16), and access control policy for IoT (P25). Liu et al. (2018) propose a privacy-preserving traffic obfuscation framework to defend smart homes against Internet traffic analysis. Next, Razeghi et al. (2017) consider a privacy preserving encoding framework for identification's applications covering biometrics, physical object security and the IoT. The proposed framework is based on a sparsifying transform, which consists of a trained linear map, an element-wise nonlinearity, and privacy amplification.

Cho et al. (2017) propose a scheme that can quantitatively evaluate the level of hiding of application programming interfaces (APIs), which represent the function of the Android application based on machine learning theory. Model for obfuscation assessment schemes was built, because it can evaluate the level of obfuscation in general without relying on specific obfuscation tools. Dynamic access control policy based on blockchain and machine learning for the IoT is presented by Outchakoucht et al. (2017). Their proposal is based on the concept of the blockchain to ensure the distributed aspect and on reinforcement learning, in order to provide a dynamic, optimized and self-adjusted security policy.

4 CONCLUSIONS

Machine learning for the IoT security is an interesting topic that is illustrated by many recent works in existing literature. Using a systematic review literature protocol described by Kitchenham and Charters (2007), we have selected and analysed 26 primary studies. Research on machine learning for IoT security has become active in 2016, so this research topic is quite new and it is quickly evolving. The number of paper significantly increased in 2017. Most of the primary studies are conference paper, but also 38% of primary studies consists of journal papers (the research on the topic has become more mature). IEEE journals and conferences are the main sources where authors publish papers on machine learning algorithms for tackling IoT security problems. Due to the number of the analysed papers and novelty of the topic, it is too early to draw decisive conclusion and make definitive predictions about the future. However, based on existing relevant primary studies we present our main conclusions as answers to research questions as follows:

RQ1: What are the most used machine learning algorithms/techniques/methods for IoT security papers? The Support Vector Machine (SVM) is most used machine learning method for IoT security in existing literature. It is used for both intrusion detection and authentication. Next method of choice is Artificial Neural Network (ANN), following by Naïve Bayes and Decision Tree.

RQ2: How can we classify machine learning for IoT security papers? We have classified the primary studies into three main categories: *intrusion detection*, *authentication*, and *other*. The category with the most of papers (62%) is *intrusion detection*, so for now, machine learning techniques were used most often for IoT intrusion detection purpose.

Our systematic literature review has shown that use of machine learning for IoT security is a new and interesting research topic. We expect that corpus of the mentioned research topic will grow in the following years. Future research can include finding new algorithms or combination of existing algorithms (hybrid models) for IoT intrusion detection to aim for a better detection rate with fewer false alarms. We also expect more works on using machine learning for privacy preservation and code obfuscation in the IoT domain. IoT security is complex research and practical problem. Machine learning is a promising technique to solve some of the IoT security problems, so we think that research topic presented in this work will be actual in the following years, and we hope this systematic literature review will help researchers to explore the state of the art and identify the possibility of interesting future research works.

ACKNOWLEDGEMENTS

This work has been fully supported by the Croatian Science Foundation under the project IP-2014-09-3877.

REFERENCES

Abeshu, A., Chilamkurti, N., 2018. Deep Learning: The Frontier for Distributed Attack Detection in Fog-to-Things Computing. *IEEE Communications Magazine 56, 169–175.* https://doi.org/10.1109/MCOM.2018.1700332

Agatonovic-Kustrin, S., Beresford, R., 2000. Basic concepts of artificial neural network (ANN) modeling and its application in pharmaceutical research. *Journal of Pharmaceutical and Biomedical Analysis 22, 717–727.* https://doi.org/10.1016/S0731-7085(99)00272-1

Ahmed, M.E., Kim, H., Park, M., 2017. Mitigating DNS query-based DDoS attacks with machine learning on software-defined networking, in: MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM). Presented at the *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM), IEEE, Baltimore, MD, USA, pp. 11–16.* https://doi.org/10.1109/MILCOM.2017.8170802

Ali, T., Nauman, M., Jan, S., 2018. Trust in IoT: dynamic remote attestation through efficient behavior capture. *Cluster Computing 21, 409–421*. https://doi.org/10.1007/s10586-017-0877-5

Aminanto, M. E., Choi, R., Tanuwidjaja, H. C., Yoo, P. D., Kim, K., 2018. Deep Abstraction and Weighted Feature Selection for Wi-Fi Impersonation Detection. *IEEE Transactions on Information Forensics and Security 13, 621–636*. https://doi.org/10.1109/TIFS.2017.2762828

Aminanto, M. E., Tanuwidjaja, H. C., Yoo, P. D., Kim, K., 2017. Wi-Fi intrusion detection using weighted-feature selection for neural networks classifier, in: 2017 International Workshop on Big Data and Information Security (IWBIS). Presented at the *2017 International Workshop on Big Data and Information Security (IWBIS), IEEE, Jakarta, Indonesia, pp. 99–104*. https://doi.org/10.1109/IWBIS.2017.8275109

Amor, N. B., Benferhat, S., Elouedi, Z., 2004. Naive Bayes vs decision trees in intrusion detection systems. *ACM Press, p. 420*. https://doi.org/10.1145/967900.967989

Baldini, G., Giuliani, R., Steri, G., Neisse, R., 2017a. Physical layer authentication of Internet of Things wireless devices through permutation and dispersion entropy, in: 2017 Global Internet of Things Summit (GIoTS). Presented at the *2017 Global Internet of Things Summit (GIoTS), IEEE, Geneva, Switzerland, pp. 1–6*. https://doi.org/10.1109/GIOTS.2017.8016272

Baldini, G., Steri, G., Giuliani, R., Gentile, C., 2017b. Imaging time series for internet of things radio frequency fingerprinting, in: *2017 International Carnahan Conference on Security Technology (ICCST). Presented at the 2017 International Carnahan Conference on Security Technology (ICCST), IEEE, Madrid, Spain, pp. 1–6.* https://doi.org/10.1109/CCST.2017.8167861

Bhunia, S.S., Gurusamy, M., 2017. Dynamic attack detection and mitigation in IoT using SDN, in: 2017 27th International Telecommunication Networks and Applications Conference (ITNAC). Presented at the *2017 27th International Telecommunication Networks and Applications Conference (ITNAC), IEEE, Melbourne, VIC, Australia, pp. 1–6*. https://doi.org/10.1109/ATNAC.2017.8215418

Canedo, J., Skjellum, A., 2016. Using machine learning to secure IoT systems, in: 2016 14th Annual Conference on Privacy, Security and Trust (PST). Presented at the 2016 14th Annual Conference on Privacy, Security and Trust (PST), *IEEE, Auckland, New Zealand, pp. 219–222*. https://doi.org/10.1109/PST.2016.7906930

Chen, F., Deng, P., Wan, J., Zhang, D., Vasilakos, A.V., Rong, X., 2015. Data Mining for the Internet of Things: Literature Review and Challenges. *International Journal of Distributed Sensor Networks 11, 431047*. https://doi.org/10.1155/2015/431047

Cho, T., Kim, H., Yi, J.H., 2017. Security Assessment of Code Obfuscation Based on Dynamic Monitoring in *Android Things. IEEE Access 5*, 6361–6371. https://doi.org/10.1109/ACCESS.2017.2693388

Diro, A. A., Chilamkurti, N., 2018. Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems 82, 761–768*. https://doi.org/10.1016/j.future.2017.08.043

Domb, M., Bonchek-Dokow, E., Leshem, G., 2017. Lightweight adaptive Random-Forest for IoT rule generation and execution. *Journal of Information Security and Applications 34, 218–224*. https://doi.org/10.1016/j.jisa.2017.03.001

Gao, S., Thamilarasu, G., 2017. Machine-Learning Classifiers for Security in *Connected Medical Devices, in: 2017 26th International Conference on Computer Communication and Networks (ICCCN). Presented at the 2017 26th International Conference on Computer Communication and Networks (ICCCN), IEEE, Vancouver, BC, Canada, pp. 1–5.* https://doi.org/10.1109/ICCCN.2017.8038507

Gebrie, M. T., Abie, H., 2017. Risk-based adaptive authentication for internet of things in smart home eHealth, in: *ECSA '17 Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings. Presented at the ECSA '17 Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings, ACM Press, Canterbury, United Kingdom, pp. 102–108.* https://doi.org/10.1145/3129790.3129801

Indre, I., Lemnaru, C., 2016. Detection and prevention system against cyber attacks and botnet malware for information systems and Internet of Things, in: *2016 IEEE 12th International Conference on Intelligent*

Computer Communication and Processing (ICCP). Presented at the 2016 IEEE 12th International Conference on Intelligent Computer Communication and Processing (ICCP), IEEE, Cluj-Napoca, Romania, pp. 175–182. https://doi.org/10.1109/ICCP.2016.7737142

Kitchenham, B., Charters, S., 2007. Guidelines for performing Systematic Literature reviews in Software Engineering Version 2.3 (Technical report No. EBSE-2007-01). *Keele University and University of Durham*.

Lee, S.-Y., Wi, S., Seo, E., Jung, J.-K., Chung, T.-M., 2017. ProFiOt: Abnormal Behavior Profiling (ABP) of IoT devices based on a machine learning approach, in: 2017 27th International Telecommunication Networks and Applications Conference (ITNAC). Presented at the *2017 27th International Telecommunication Networks and Applications Conference (ITNAC), IEEE, Melbourne, VIC, Australia, pp. 1–6.* https://doi.org/10.1109/ATNAC.2017.8215434

Liu, J., Zhang, C., Fang, Y., 2018. EPIC: A Differential Privacy Framework to Defend Smart Homes Against Internet Traffic Analysis. *IEEE Internet of Things Journal 1–1.* https://doi.org/10.1109/JIOT.2018.2799820

Mahdavinejad, M. S., Rezvan, M., Barekatain, M., Adibi, P., Barnaghi, P., Sheth, A. P., *2017. Machine learning for Internet of Things data analysis: A survey. Digital Communications and Networks.* https://doi.org/10.1016/j.dcan.2017.10.002

Nobakht, M., Sivaraman, V., Boreli, R., 2016. A Host-Based Intrusion Detection and Mitigation Framework for Smart Home IoT Using OpenFlow, in: 2016 11th International Conference on Availability, Reliability and Security (ARES). Presented at the 2016 11th International Conference on Availability, Reliability and Security (ARES), *IEEE, Salzburg, Austria, pp. 147–156.* https://doi.org/10.1109/ARES.2016.64

Outchakoucht, A., Es-Samaali, H., Philippe, J., 2017. Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things. *International Journal of Advanced Computer Science and Applications 8.* https://doi.org/10.14569/IJACSA.2017.080757

Perez, D., Astor, M.A., Abreu, D.P., Scalise, E., 2017. Intrusion detection in computer networks using hybrid machine learning techniques, in: 2017 XLIII Latin American Computer Conference (CLEI). Presented at the *2017 XLIII Latin American Computer Conference (CLEI), IEEE, Cordoba, Argentina, pp. 1–10.* https://doi.org/10.1109/CLEI.2017.8226392

Razeghi, B., Voloshynovskiy, S., Kostadinov, D., Taran, O., 2017. Privacy preserving identification using sparse approximation with ambiguization, in: *2017 IEEE Workshop on Information Forensics and Security (WIFS). Presented at the 2017 IEEE Workshop on Information Forensics and Security (WIFS), IEEE, Rennes, France, pp. 1–6.* https://doi.org/10.1109/WIFS.2017.8267664

Roux, J., Alata, E., Auriol, G., Nicomette, V., Kaaniche, M., 2017. Toward an Intrusion Detection Approach for IoT Based on Radio Communications Profiling, in: *2017 13th European Dependable Computing Conference (EDCC). Presented at the 2017 13th European Dependable Computing Conference (EDCC), IEEE, Geneva, Switzerland, pp. 147–150.* https://doi.org/10.1109/EDCC.2017.11

Wang, L. (Ed.), 2005. Support vector machines: theory and applications, Studies in fuzziness and soft computing. *Springer, Berlin*.

Wang, Z., Chen, Y., Patil, A., Jayabalan, J., Zhang, X., Chang, C.-H., Basu, A., 2017. Current Mirror Array: A Novel Circuit Topology for Combining Physical Unclonable Function and Machine Learning. *IEEE Transactions on Circuits and Systems I: Regular Papers 1–13*. https://doi.org/10.1109/TCSI.2017.2743004

Wu, M., Song, Z., Moon, Y.B., 2017. Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods. *Journal of Intelligent Manufacturing.* https://doi.org/10.1007/s10845-017-1315-5

Yeh, K.-H., Su, C., Hsu, C.-L., Chiu, W., Hsueh, Y.-F., 2016. Transparent authentication scheme with adaptive biometrie features for IoT networks, in: 2016 IEEE 5th Global Conference on Consumer Electronics. Presented at the *2016 IEEE 5th Global Conference on Consumer Electronics, IEEE, Kyoto, Japan, pp. 1–2*. https://doi.org/10.1109/GCCE.2016.7800550

Zissis, D., 2017. Intelligent security on the edge of the cloud, in: *2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC). Presented at the 2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC), IEEE, Funchal, Portugal, pp. 1066–1070.* https://doi.org/10.1109/ICE.2017.8279999