Bagaa, Miloud; Taleb, Tarik; Bernabe, Jorge Bernal; Skarmeta, Antonio

A Machine Learning Security Framework for Iot Systems

Published in:
IEEE Access

DOI:
10.1109/ACCESS.2020.2996214

Published: 01/01/2020

Document Version
Publisher's PDF, also known as Version of record

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 27, 2020, accepted May 8, 2020, date of publication May 21, 2020, date of current version June 30, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2996214

A Machine Learning Security Framework for Iot Systems

MILOUD BAGAA[1], (Member, IEEE), TARIK TALEB[1,3,4], (Senior Member, IEEE), JORGE BERNAL BERNABE[2], AND ANTONIO SKARMETA[2], (Member, IEEE)

[1]Department of Communications and Networking, School of Electrical Engineering, Aalto University, 02150 Espoo, Finland
[2]Department of Communications and Information Engineering, University of Murcia, 30001 Murcia, Spain
[3]Department of Computer and Information Security, Sejong University, Seoul 05006, South Korea
[4]Centre for Wireless Communications (CWC), University of Oulu, 90570 Oulu, Finland

Corresponding author: Miloud Bagaa (miloud.bagaa@aalto.fi)

This work was supported in part by the European Research Project H2020 ANASTACIA under Grant GA 731558, in part by the H2020 INSPIRE-5Gplus Project under Grant GA 871808, in part by the AXA Postdoctoral Scholarship awarded by the AXA Research Fund (Cyber-SecIoT project), in part by the Academy of Finland 6Genesis Project under Grant 318927, and in part by the Academy of Finland CSN Project under Grant 311654.

ABSTRACT Internet of Things security is attracting a growing attention from both academic and industry communities. Indeed, IoT devices are prone to various security attacks varying from Denial of Service (DoS) to network intrusion and data leakage. This paper presents a novel machine learning (ML) based security framework that automatically copes with the expanding security aspects related to IoT domain. This framework leverages both Software Defined Networking (SDN) and Network Function Virtualization (NFV) enablers for mitigating different threats. This AI framework combines monitoring agent and AI-based reaction agent that use ML-Models divided into network patterns analysis, along with anomaly-based intrusion detection in IoT systems. The framework exploits the supervised learning, distributed data mining system and neural network for achieving its goals. Experiments results demonstrate the efficiency of the proposed scheme. In particular, the distribution of the attacks using the data mining approach is highly successful in detecting the attacks with high performance and low cost. Regarding our anomaly-based intrusion detection system (IDS) for IoT, we have evaluated the experiment in a real Smart building scenario using one-class SVM. The detection accuracy of anomalies achieved 99.71%. A feasibility study is conducted to identify the current potential solutions to be adopted and to promote the research towards the open challenges.

INDEX TERMS Internet of Things, security, artificial intelligence, SDN, NFV, orchestration and MANO.

I. INTRODUCTION

The disruptive acceleration of Internet of Things (IoT) is drastically modifying the current ICT landscape with a massive number of cellular IoT devices expected to be deployed in the next few years. IoT devices are taking over a variety of aspects of our current lives, such as health care, transportation, and home environments [1]. Thanks to the massive growth in analytics and cloud computing technologies, they are expected to be able to provide relevant contextual data using their autonomous communication with each other without human interaction. All of these envisioned benefits are rapidly pushing the adoption of this technology. On the other side of the spectrum, IoT nodes can be comprised by malicious attackers leveraging their resource constraints and relevant vulnerabilities. Accounting for their wide adoption, IoT security threats can cause severe privacy problems and economical damage. As they are becoming an essential element in our daily lives, maintaining privacy, security and business operations/opportunities are of a very high priority. For instance, IoT devices could be used for various purposes and can be deployed in different places including home, health care and industrial environments. Thus, they can carry sensitive personal data, such as user information and daily activities. An attack against those IoT devices could lead to sensitive information leakage and can cause an interruption in workflows, thus compromising the quality of the products. In order to accommodate the constraints and heterogeneity of

The associate editor coordinating the review of this manuscript and approving it for publication was Moayad Aloqaily.

IoT systems, softwarized networks seem to be the most compelling solution. Network softwarization is a recent promising trend aiming at radically advancing telecommunication industries by embracing cloud computing technologies and software models in network services [2].

The main pillars behind this revolution are SDN and NFV. On one hand, SDN introduces a new level of network programmability by decoupling control and data plane. A logically centralized controller is in charge of supervising the network state and provides rules to the network elements for appropriately managing the traffic flows. On the other hand, NFV leverages virtualization technologies to deploy network elements as software instances, thus allowing an increased level of flexibility and elasticity in service provisioning. Furthermore, NFV can enable a remarkable reduction in CAPEX/OPEX costs by replacing dedicated expensive hardware with commodity servers able to host software-based network appliances. Although SDN and NFV are two separate paradigms, their joint use can further improve the potential security services offered by the network and meet the broad range of increasing requirements imposed by novel IoT applications. The explosive number of expected IoT devices, the widespread diffusion of location-based mobile gaming applications, the tactile Internet applications are all significant representatives of demanding scenarios which expose a wide range of new vulnerabilities and security concerns. Leveraging the flexibility and scalability offered by the integration of SDN and NFV, the telco operators will successfully be able to enforce the relevant security policies in the IoT domain [3]. In this fervent context, several works have already investigated models to implement Security-as-a-Service (SECaaS) [4], [5].

Industrial and research communities are boosting great efforts to implement similar models within the IoT network domain by leveraging SDN and NFV features. On the other hand, the fast growing number of IoT attacks demands for an adaptive framework which can deal with unknown types of attacks using different monitoring inputs. The new services and features introduced into the IoT system exposes new and unseen types of vulnerabilities. In this context, machine learning is very compelling. State of the art AI algorithms make use of machine learning to identify attacks as well as adapt and respond to new potential cybersecurity risks by classifying attacks depending on their threat level. Moreover, when deep machine learning principles are incorporated into the system, they can actually adapt over time, giving an edge to the network administrators over the cybercriminals [6]. Intrusion detection in IoT, unlike traditional infrastructures, should consider not only network-systems metrics but also processes and measurements from the physical environment.

This paper provides a complete framework that leverages machine learning (ML) techniques and 5G enabling technology SDN, NFV and IoT controllers for efficiently and fast detecting and preventing cybersecurity attacks. The contributions of the paper are many fold:

- A unified AI security framework that is aligned with ETSI ZSM [7] vision by monitoring, detecting and preventing cybersecurity threats in a closed-loop automation, autonomous and harmonized way;
- Implemention and validation of an AI security framework for IoT that exploits machine learning techniques in order to deal with, not only knowledge-based intrusion detection through network patterns/signatures recognition, but also anomaly-based intrusion detection based on deviations from the normal behavior of devices, whose reported data are observed by the monitoring capabilities of the framework;
- Three approaches have been suggested that leverage ML techniques for detecting cybersecurity attacks based on the network patterns;
- The unified AI security framework is empowered with abilities to identify new kind of cyberattacks (0-days attacks) in IoT, which could not be detected otherwise by means of network pattern recognition;
- Leveraging SDN/NFV-based security management features to dynamically and efficiently mitigate the detected cyberattacks, according to the AI-based contextual decisions inferred by the framework;

Besides, the SDN/NFV-based security management features of the framework permit a dynamic and efficient mitigation of the detected cyberattacks, according to the AI-based contextual decisions inferred by the framework.

The rest of paper is organized as in the following. In Section II, we provide a summary of related work in the literature. The framework architecture and related technologies are described in Section III. Section IV presents the performance evaluation results of the AI agents in the two approaches. Finally, Section V Concludes the work and highlights the open challenges.

II. RELATED WORKS

The IoT security is a fervent research area which attracts a rising amount of attention from the research community. There have been many works covering this important aspect. For instance, authors in [8] have presented an IoT security framework for smart infrastructures, such as smart homes and smart buildings. It employs continuous monitoring to capture the sensor's operational data in order to detect abnormal behavior in IoT domain. This data is used to identify the sensor and compare its behavior to ''normal'' behavior. If an attack is detected, it classifies it according to the type of abnormality and takes relevant recovery actions, such as sensor re-authentication, discarding the sensor's data or changing the network configuration. Although the results show that the system is able to provide high levels of accuracy in terms of detecting the attacks, the possible mitigation actions are very limited and often causes service disruptions. Moreover, the platform does not provide E2E (End to End) security, which is a must have as the attacks can target any layer of the IoT framework.

The flexibility of SDN have been leveraged in the works [9], [10] by defining SDN-based security frameworks. The extra functionalities offered by SDN technology enable the integration of new security tools, such as fine grained routing manipulations, traffic filtering and the use of secure network channels to transfer sensitive data. While in the NFV scope, several research papers focused on evaluating the performance and feasibility of running virtual security appliances on the edge using containers [11], [12] such as Intrusion Detection Systems (IDS) and firewalls. Although this lighter virtualization technology showed great efficiency, it turned out to be challenging accounting for the resource-constrained IoT devices. Indeed, the high amount of traffic can yield to high energy and CPU consumption, thus affecting the device's usability. An alternative approach to secure the IoT systems is to use machine learning techniques. Different solutions that leverage SDN technology and ML techniques for enabling network intrusion detection systems have been suggested in [13]. The work also describes the implementation challenges related to the implementation of network intrusion detection systems.

Authors in [14] have proposed a solution that predicts the city buses location using a deep learning approach. In the proposed solution, Long–Short Term Memory (LSTM) based neural network has been considered for predicting the locations and data rate. Authors in [15] have presented a solution that leverages block-chain for managing scalable IoT systems. Authors in [16] have suggested a solution that secures the communications between IoT devices and the MEC. The proposed solution adopts a learning method to identify candidates for service composition and delivery. Authors in [17] have investigated the use of Artificial Neural Networks in order to detect abnormal network traffic going from the gateway to the edge devices [18]. In their approach, they used temperature sensors as edge devices and a Raspberry Pi as an IoT gateway. The system collects multiple data samples from the edge devices and stores them in a database on the gateway. Then, they split these inputs into training and testing data. Once the neural network has been trained using the training data, the testing data is used to evaluate the accuracy of the model. Although the results show an improved level of security in terms of anomaly detection, the capability of this system was hindered by the limited resources on the IoT gateway affecting the user experience and the lifespan of the device negatively in the process. An intrusion detection system running on top of connected vehicles has been suggested in [19]. The suggested framework adapts deep belief and decision tree machine learning mechanisms for detecting different attacks.

AI can leverage Intrusion detection systems (IDS) for IoT, thereby detecting anomalous behaviors based on metrics coming from both, network-systems as well as physical measurements reported by IoT devices. Mehta *et al.* [20] provide an AI-based IDS method for IoT that exploits the relationship between a set of given time-series of sensor data for detecting anomalies. Nonetheless, our AI framework is intended to cope with not only anomalous-based IDS [21], but also knowledge-based IDS, by checking continuously signatures and patterns of previously known vulnerabilities and attacks [22]. In this regard, most of the research work done so far has been focused on the incident detection phase. Our framework aims to cover also the reaction stage, once the attack has been identified.

We strongly believe that an ideal solution would guarantee an End-to-End security thanks to the global network vision of the SDN controller, and a proper security policy definition and refinement using AI. This relevant security policy would be enforced thanks to the advanced functionalities offered by virtual network security appliances hosted on the cloud. Therefore, we introduce our novel AI-based security framework for IoT systems.

III. PROPOSED FRAMEWORK

A. BACKGROUND ON TECHNOLOGIES

1) SOFTWARE DEFINED NETWORKING (SDN)

SDN is a relatively new paradigm that aims to decouple the control plane from the data plane for increasing the network flexibility and programmability, as well as the manageability, allowing external application to control the network's behavior in an easy and efficient way. SDN offers novel capabilities to adapt on-the-fly the network flows according to the dynamic application requests. The three main components of SDN-enabled network are: switches, controllers, and communication interfaces, where the SDN controller is a centralized entity that enforces the cognitive decisions in the switches, maintains the state of the whole system, e.g. it decides on the traffic routing by updating relevant flow rules on the switches.

The adoption of SDN in IoT (SDN-enabled IoT systems) is considered an essential element in the success and feasibility of future IoT systems. Leveraging SDN through its intelligence in routing the traffic and optimizing the network utilization are key enabling functions to manage the massive amounts of data flow in IoT networks and eliminate bottlenecks [23]. This integration can be implemented at different levels of the IoT network, such as the access (where the data is generated), core and cloud networks (where the data is processed and served), which enables IoT traffic management from end-to-end.

Moreover, SDN can be also leveraged to provide advanced security mechanisms for IoT systems. For example, traffic isolation between different tenants, centralized security monitoring using the global vision of the network and traffic dropping at the edge, keeping the malicious traffic from spreading all over the network.

2) NETWORK FUNCTION VIRTUALIZATION

Network Function Virtualization (NFV) refers to the adoption of virtualization technologies in network environments. Unlike traditional network equipment, NFV decouples the software from the hardware, bringing value-added features

and notable capital and operating expenditures gains. The ETSI (European Telecommunications Standards Institute) has been leading the standardization of this approach, defining novel architecture that enables the aforementioned advantages.

The ETSI NFV architecture identifies three main building blocks:

1) Virtualization Infrastructure: This layer includes all the hardware and virtualization technologies necessary to provide the desired resource abstractions for the deployment of Virtualized Network Functions (VNFs). This includes storage, compute and networking resources, which are usually managed by a cloud platform.
2) Virtual Network Functions: The core idea of NFV deals with replacing dedicated hardware equipment with software-based instances of network functions, i.e., the VNFs. They can be deployed and managed over multiple environments, providing scalable and cost-effective network functions.
3) Management and Orchestration: The NFV management and orchestration (MANO) block interacts with both the infrastructure and VNF layers in the ETSI NFV architecture. It is responsible for the management of the global resource allocation that includes: instantiating, configuring and monitoring VNFs.

Introducing virtualized network resources into the IoT ecosystem brings multiple value-added features, accounting for their heterogeneity and rapid growth. When coupled with SDN, NFV can not only, provide advanced virtual monitoring tools, such as Intrusion Detection Systems (IDSs) and Deep Packet Inspectors (DPIs), but also provision, and configure on-demand and scalable network security appliances, such as firewalls and authentication systems, in order to cope with the attacks detected by the monitoring agents [24], [25]. Moreover, offloading the extra processing induced by security from these resource-constrained IoT devices to virtual instances [26] saves energy and improves efficiency leaving more headroom to other useful applications. The aforementioned flexibility and advanced security features of NFV are lacking in current out-the-shelf IoT security hardware. Although NFV is not aiming to completely replace current IoT solutions, its complementary value added features turned out to be very compelling and revolutionizing in the IoT security landscape.

3) MACHINE LEARNING TECHNIQUE

Machine learning (ML) is a field of artificial intelligence that integrates a set of techniques and algorithms to provide intelligence to computers and smart devices. ML techniques, such as supervised learning, unsupervised learning, and reinforcement learning, have been widely adopted in the network security landscape. It is employed in order to accurately detect and define the specific security policies to enforce in the data plane. The challenge is to fine-tune the different parameters of relevant security protocols in order to mitigate a certain type of attack either by labeling the network traffic or defining access control policies. Indeed, different ML techniques can address a variety of IoT attacks. For example, neural networks can be used to detect network intrusion [27] and DoS attacks and K-NN in malware detections [28].

1) Supervised Learning: In supervised algorithms, the inner relations of the data may not be known, but the output of the model is. Usually, the training of this model requires a set of data to ''learn'' and other to test and evaluate the dirved model. A common example in the security landscape is matching an attack pattern to a set of already known attacks.
2) Unsupervised Learning: Unlike supervised learning approach, in unsupervised learning technique, the model is unknown, meaning that the data does not have to be labeled. Relevant types of models try to find a correlation between the data and classify it into different groups.
3) Reinforcement Learning: Reinforcement learning focuses on studying the problems and techniques that try to improve its model. It has a unique model training method, it uses trial and error and reward functions. It monitors the results of its output and calculates a value called ''value function'' using the reward. According to this value, the model knows the accuracy of its decision and adapts itself accordingly.

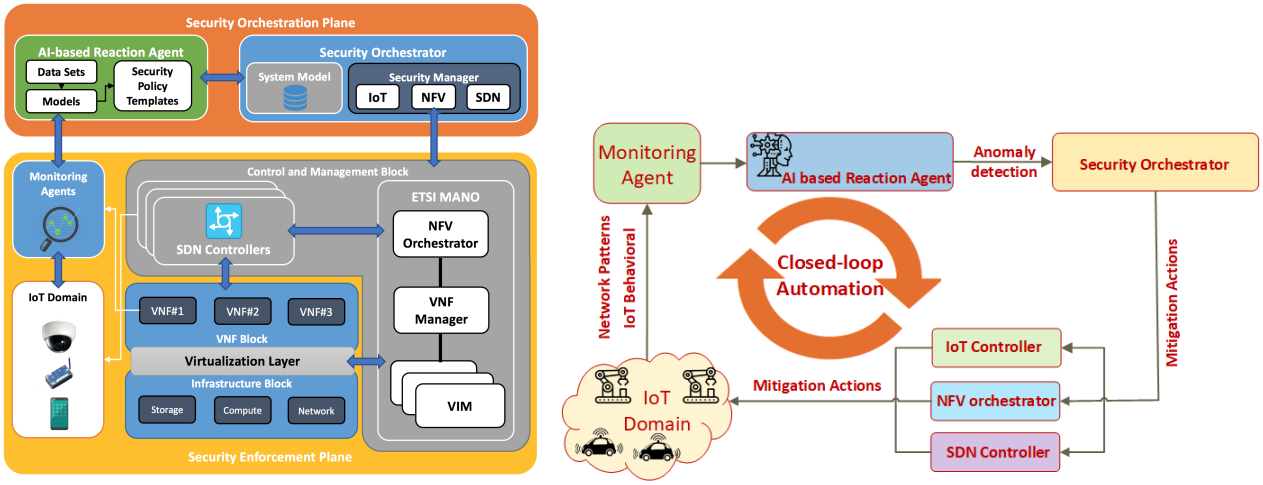
B. FRAMEWORK OVERVIEW

To cope with the different security problems associated with IoT systems, we propose a security framework combining SDN, NFV and ML, depicted in Figure 1. While Figure 1(a) shows the components and their interactions in the proposed security framework, Figure 1(b) shows the closed-loop automation proposed in this paper from monitoring and detection to attack mitigation. The proposed system provides comprehensive security by integrating the countermeasures and enablers discussed in the previous subsections. This framework allows the enforcement of security policies, from their design to their deployment and maintenance.

As depicted in Figure 1(a), the framework consists of two main layers: *i*) Security Orchestration Plane; *i*) Security Enforcement Plane. In what follow, we will describe these two planes, as well as their inter and intra communications for ensuring the closed loop automation for detecting and mitigating different threats.

1) SECURITY ENFORCEMENT PLANE

The communication between the IoT devices and end-users happens thanks to different VNFs deployed on different clouds and edges and physical network functions (PNFs). The communication between these network functions (i.e., VNFs and PNFs), IoT devices and end-users happens via legacy network or SDN-based network. In IoT domain, we distinguish between two types of attacks, which are internal and



(a) General Architecture of the Framework

(b) Closed-loop Automation: From Detection to Mitigation

FIGURE 1. Proposed Framework Main Overview.

external attacks. While the latter is launched at the end-user (i.e., external) network towards the IoT domain (i.e., internal) network, the former happens due to malicious and intruder IoT devices. The latter generates attacks either towards other legitimate IoT devices and/or the external network. Mainly, the attacks would be mitigated at the level of: *i*) The IoT devices by leveraging IoT controllers; *ii*) The network level by leveraging SDN controllers; *iii*) The cloud/MEC level by leveraging NFV orchestrator.

The security properties defined by the framework should be appropriately enforced within the IoT domain, by deploying security VNFs and configuring the connectivity via SDN networking. The security enforcement plane is designed to be fully compliant with SDN/NFV standards, as specified by ETSI NFV and ONF (Open Networking Foundation) SDN specifications, respectively. The envisaged security enforcement countermeasures will involve three logical blocks as depicted in Fig. 1(a).

a: VNF BLOCK

accounts for the VNFs deployed over the virtualization infrastructure to enforce security using different network services. Specific attention will be addressed to the provisioning of advanced security VNFs (such as virtual firewall, IDS/IPS, etc.) that should be able to provide the protection and threat countermeasures requested by the security policies.

b: CONTROL AND MANAGEMENT BLOCK

considers the components required to manage both SDN and NFV environments. To this objective, it includes the ETSI MANO stack modules and SDN controllers. Since NFV is usually combined with SDN to programmatically adjust the network according to the resources and policies, tight interaction is expected between the NFV orchestrator and the SDN controllers to enable the deployment of appropriate security functionalities.

c: INFRASTRUCTURE BLOCK

comprises all the physical machines capable of providing computing, storage, and networking capabilities to build an Infrastructures as a Service (IaaS) layer by leveraging appropriate virtualization technologies. This plane also includes the network elements responsible for traffic forwarding, following the SDN controller's rules, and a distributed set of security probes for data collection to support the monitoring services.

d: MONITORING AGENTS

are mainly responsible for reporting network traffic and IoT behaviors for detecting different attacks. The detection mechanism, in the proposed framework, can be either using network patterns or IoT misbehavior. They will be aware of all the traffic flowing through the network thanks to the traffic mirroring done through SDN. Each monitoring agent sends the logs containing the description of the relevant suspicious activities to the AI-based reaction agent hosted in the Security Orchestration Plane.

e: IoT DOMAIN

stands for the SDN-enabled network of physical devices varying from security cameras, temperature sensors, home appliances to any other smart devices exchanging data. Accounting for the high vulnerability of these devices, our framework aims to enforce the security policies in this domain in order to ensure data privacy and integrity.

2) SECURITY ORCHESTRATION PLANE

This plane is responsible for the run-time configuration of the security policies and their context-aware refinement based on up-to-date monitoring data. It is an innovative layer of our

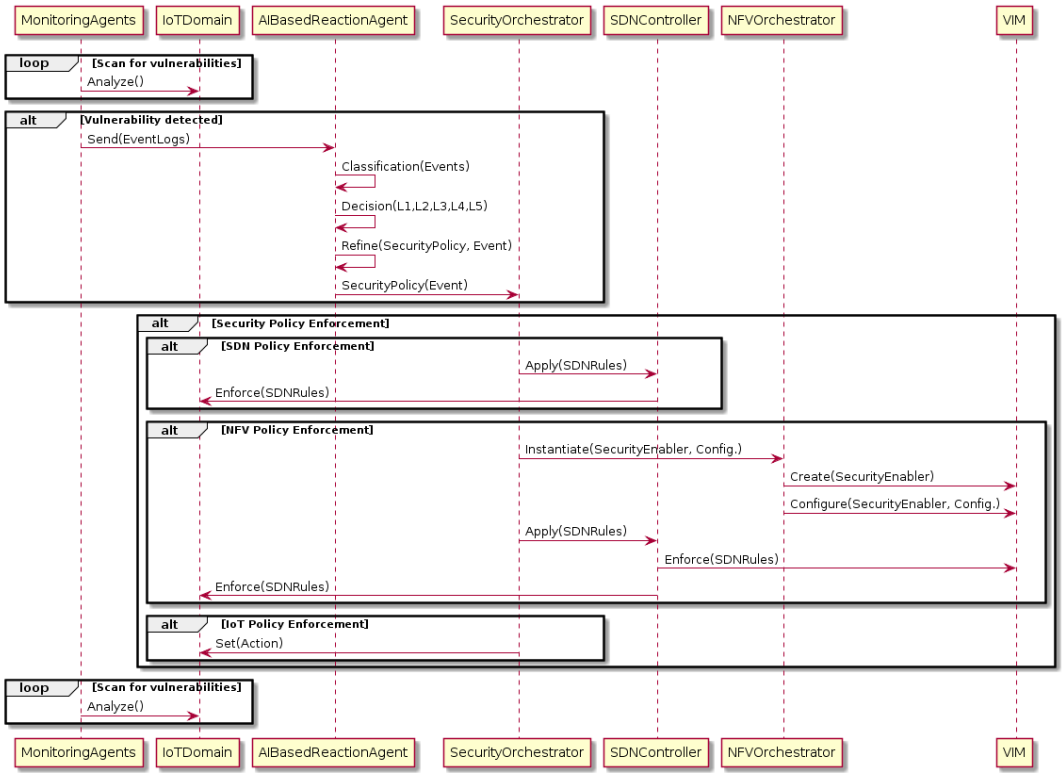


FIGURE 2. Overview of the interactions between the components of the AI-based Security Framework for IoT Systems.

architecture and responsible for enforcing relevant security policies into the IoT domain by making the relevant requests to the Security Enforcement Plane. This includes instantiating, configuring and monitoring different virtual security enablers in order to cope with the current attack.

The main interactions can be seen in the diagram depicted in Figure 2 that summarizes the different interactions between the component of our framework. As depicted in Figures 1(b) and 2, a closed loop automation mechanism is proposed in this paper starting from the monitoring agent, AI based reaction agent to the security orchestrator. The latter mitigates the threats via IoT controller, SDN controller and NFV Orchestrator, respectively.

a: AI-BASED REACTION AGENT

This component is responsible for dictating the mitigation actions to be taken by the Security Orchestrator. As depicted in Figure 1(b) and the first block in Figure 2, this component uses the data collected from the network and IoT domains thanks to the monitoring agent. This component uses a trained machine learning models based on network patterns and IoT behaviors for detecting threats. These machine learning models will be able to dictate the appropriate security policy template that should be sent to the security orchestrator. As depicted in Figure 1(b) and second block in Figure 2, the security threats are detected based on IoT behaviors and/or network patterns. Then, the threat level (Each level - L1, L2,L3,L4,L5- corresponds to a pre-defined security policy), would be identified and sent to the security orchestrator.

As depicted in Figure 1(b), AI based reaction agent uses different Machine learning Algorithms, including J48, Byes Net, RandomForest, Hoeffding, support vector machine (SVM) and deep learning, for detecting different attacks related IoT behaviors and/or network patterns. More information about the implementation of this component would be provided in section IV.

b: SECURITY ORCHESTRATOR

This component is one part of the closed-loop automation that is accountable for enforcing the security policies defined by the AI Reaction Agent. It interacts with the Control and Management Block in order to enforce the relevant security policies using SDN and NFV in the IoT domain. As depicted in the third block in Figure 2, the security orchestrator proceeds either by instantiating, configuring and then monitoring virtual security appliances or manipulating the malicious traffic using SDN or even taking direct actions on the IoT devices themselves, such as turning off a compromised device. The Security Orchestrator also houses a System Model database which contains all the information related to the data plane and enforced policies, such as the reaction agent requests, SDN controllers and switches, current running VNFs along with their configuration and IoT device related information as well.

C. IMPLEMENTATION TOOLS

In this sub-section, we carry out an assessment study for the potential implementation of our proposed solution. To this aim, we provide an overview of the envisioned open source projects that are used for enabling the suggested framework.

1) ONOS SDN CONTROLLER

ONOS (Open Network Operating System) is an open source project that aims to create an SDN operating system for communications and service providers. It is well known for its high performance, scalability and high availability. It uses standard protocols, such as OpenFlow and NetConf in order to expose advanced traffic manipulation functions through its applications. These applications provide a high level of abstractions while giving detailed information about the network, such as existing nodes, the number of packets of a certain traffic and existing links, making application development much simpler.

2) ETSI OPEN SOURCE MANO (OSM)

OSM is an NFV Orchestrator that was officially launched at the World Mobile Congress (WMC) in 2016, founded by Mirantis, Telefnica, BT, Canonical, Intel, RIFT.io, Telekom Austria Group, and Telenor. It is compliant with the ETSI NFV MANO reference architecture and offers support for multi-cloud and SDN vendors support (OpenStack, AWS, ONOS, Opendaylight..). It is comprised of three basic components:

- The Service Orchestrator (SO): responsible for end-to-end service orchestration and provisioning, it offers a web interface and a catalog which holds the different NFV descriptors.
- The Resource Orchestrator (RO): is used to provide services over a particular IaaS provider in a given location. It interacts directly with the VIM in order to instantiate virtual resources
- The VNF Configuration and Abstraction (VCA): performs the initial VNF configuration and constant monitoring using Juju Charms LXD containers.

IV. AI-BASED REACTION AGENT IMPLEMENTATION AND PERFORMANCE EVALUATION

This section provides the experiment setup and the evaluation analysis of AI based reaction agent (detailed in subsection III). AI based reaction agent detects the threats by: *i*) Analysing the network patterns as presented in subsection IV-A. A knowledge-based intrusion detection framework is proposed for detecting different network attacks; *ii*) Analysing the anomaly behaviors in the IoT system as explained in subsection IV-B. In this subsection, the cyber-attacks are detected based on the analysis of anomaly behaviors in the IoT system.

We have used supervised learning algorithms in order to accurately classify the level of the attacks and correctly choose the appropriate security templates. Using the relevant inputs from the monitoring agents, the AI-based reaction agent will make use of multiple machine learning techniques in order to mitigate a given threat.

A. NETWORK PATTERNS ANALYSIS

The evaluation of an intrusion system is a primordial step towards proving the efficiency of the framework. There are several data sets widely used for this purpose, such as DARPA [29], KDD99 [30] and DEFCON [31]. We build IDS based on NSL KDD dataset that contains more than twenty attacks, such as Neptune-dos, pod-dos, smurfdos, buffer-overflow, rootkit, satan, teardrop, etc. The NSL KDD is an improvement of the original dataset Kdd99 that suffers from significant problems that may lead to inefficient evaluation of an IDS. Based on a work done on [32] the new NSL KDD dataset solved several serious problems, in which it eliminates about 77 of redundant records. For this reason, to design our AI-based reaction agent, we have used NSL KDD dataset.

In order to perform the evaluation of the IDS based on NSL-KDD dataset, we use a pre-processing and visualization data mining tool called Weka. Weka is used to perform classification of the training sample. The KDD dataset contains 125943 connection and 41 features, in which each sample belongs to one of the following attacks: Denial of Service Attack (DoS), User to Root Attack (U2R), Remote to Local Attack (R2L), and Probing Attack.

The variety of attributes nature makes the learning not possible for some machine learning algorithms. When an attribute is continuous, it makes the model building difficult. Hence, the preprocessing step is primordial before building classification patterns in order to maximize the predictive accuracy [33]. In particular, a discretization method is employed to tackle this limitation. The discretization is a data mining technique that aims to reduce the number of values of a continuous variable by grouping them into intervals. In literature, there are two discretization types that can be applied [34]:

- Static variable discretization: The discretization is performed one variable independently of other variables.
- Dynamic variable discretization: All attributes (variable) are simultaneously discretized.

In addition to the discretization, we also grouped the attacks in a way to only have the main attack categories (DDoS, Probe, U2R, R2L).

1) Performance comparison measurements: The evaluation of the intrusion detection system is a fundamental problem, and it is important to select the metrics that can describe the strength of the IDS [35]. The performance of an IDS is beyond the classification rate separately. We evaluate our system based on model accuracy, detection rate, precision and Cost Per Example (CPE). The following metrics employed together are essential when measuring the performances.

$$CPE = \frac{1}{N} \sum_{i=1}^{5} \sum_{j=1}^{5} CM(i,j) + C(i,j) \qquad (1)$$

TABLE 1. Cost Matrix for NSL-KDD dataset [36].

	DoS	U2R	U2L	Probe	Normal
DoS	0	2	2	1	2
U2R	2	0	2	2	3
U2L	2	2	0	2	4
Probe	2	2	2	0	1
Normal	2	2	2	1	0

TABLE 2. Detailed Precision values for each attack.

	J48	Byes Net	RandomForest	Hoeffding Tree
DoS	99.9%	99.9%	100%	99.3%
U2R	70.0%	4.8%	82.1%	11.5%
U2L	97.5%	62.7%	99.3%	35.2%
Probe	99.4%	84.2%	99.9%	98.1%
Normal	99.8%	97.3%	99.9%	95.2%
Time(s)	35.35	6.97	74.94	5.1
Precision	99.8%	96.7%	99.9%	96.4%
FPR	0.2%	1.8%	0.1%	3.3%
Detection Rate	99.8%	95.7%	99.9%	96.8%
CPE	0.47%	6.8%	0.23%	7.46%

Equation 1 represents the Cost Per Example (CPE), for some works it is referred as Cost-Sensitive Classification
(CSC) [37]. It is an important metric in order to find the cost of misclassification for intrusion detection system. Where CM is the Confusion Matrix of the classification model, C corresponds to the Cost Matrix represented in Table 1 and N represents the total number of samples. In the following, we propose different systems based on artificial intelligence. We evaluate our systems based on 10-fold cross-validation using an i5-8350U computer with 16Go RAM.

2) Preprocessing, Feature Selection and Classification: Initially, we propose a first approach that consists of preprocessing then classifying the whole dataset using different algorithms (J48, Bayes Net, Random Forest, and Hoe ding Tree). Then, we have selected the best Algorithm that gives us better performences.
3) Back-propagation technique: In the following, we explore a technique based on a multilayer neural network using a backpropagation learning algorithm. The multilayer neural network consists of three layers. The first layer is the input layer contains 41 inputs (dataset features). The last layer provides the classification answers (Dos, Probe, U2R, R2L, Normal) and additional hidden layer used for the learning process.
In this technique, we consider one hidden layer and 100 neurons. These parameters are obtained by experience, as other values of the number of hidden layer and the number of neurons, did not seem to show any significant improvements in terms of Mean Squared Error (MSE).
4) Distributed classification system: In the following, we present a distributed classification system in which we assign each attack category (DDoD, Probe, R2L, and U2R) to JRip algorithm. Then, the obtained models are merged adopting AdaBoost algorithm.

TABLE 3. Back-propagation evaluation metrics.

	DoS	U2R	U2L	Probe	Normal	Model
Precision	99.1%	0%	81.6%	99.1%	98.7%	98.7%
FPR	0.5%	0%	0.1%	0.1%	1.5%	1.0%
Detection Rate	99.0%	0%	71.5%	98.9%	99.0%	98.7%
CPE	-	-	-	-	-	2.78%
Time(s)	-	-	-	-	-	9691.01

TABLE 4. AdaBoost evaluation metrics.

	DoS	U2R	U2L	Probe	Normal	AdaBoost
Precision	100%	76.9%	99.1%	99.9%	99.9%	99.8793%
FPR	0%	0%	0%	0%	0.2%	0.1%
Detection Rate	100%	57.7%	96.7%	99.6%	99.9%	99.9%
CPE	-	-	-	-	-	0.26%
Time(s)	-	-	-	-	-	193.6

5) Results discussions:
The results presented in table 2 show that the random forest Algorithm performed well in terms of overall accuracy and model precision. Though, it shows a very low precision for U2R and R2L attacks. J48 detects attacks with very good accuracy and low miss-classification rate (or CPE). Nevertheless, J48 is not efficient in terms of precision for the U2R attacks. Hoeffding tree algorithm shows stable performance, but it also suffers from low precision for U2R attacks. In particular, Bayes Net algorithm shows the worst results as it could not recognize mostly U2R attack despite the good model accuracy.
The back-propagation system shows a slight improvement comparing to the previous approaches in terms of accuracy, precision (Table 3). However, the cost of misclassified is a little bit high as for the processing time.
AdaBoost (Table 4) obtained an enhanced model in terms of detection accuracy, detection rate and the Cost per Example (CPE).
6) Comparative Study: Table 5 shows the performance results. Compared to the previous systems, this system obtained an enhanced model in terms of detection accuracy, precision, detection rate and the Cost per Example (CPE).
We conducted a comparison with recent works based on the accuracy, the detection rate, the false positive rate, and the CPE if provided. Recent works are summarized in Table 5. The comparison results illustrate that our system based distributed JRip algorithm and ensemble method is the best while the results of our other systems are also promising. Those systems, namely, the Filter-based Support Vector Machine (F-SVM) [38], Dirichlet Mixture Model (DMM) [39], Triangle Area Nearest Neighbors (TANN) [40], Deep Belief Networks (DBN) [41], Recurrent Neural Network (RNN) [42], Deep Neural Network (DNN)

TABLE 5. Results comparison with previous work.

	Accuracy	Detection rate	FPR	Training Time
L-SSVM [38]	92.29%	92.2%	0.41%	-
DMM [39]	97.8%	97.8%	2.5%	-
TANN [40]	96.91%	97.8%	2.5%	-
DBN [41]	97.45%	-	-	3.2 sec
RNN [42]	99.53%	97.09%	3.6%	5516 sec
DNN [43]	75.75%	75%	15%	-
E-DNN [44]	92.49%	98%	14.7%	-
DFF-NN [45]	98.6%	99%	1.8%	398 sec
DL [46]	98%	71%	-	-
SVM-DR [46]	97.61%	97.27%	-	-
Our Approach1	99.8%	98.8%	0.2%	35.35
Our Approach2	98.7%	98.7%	1.0%	9691.01
Our Approach3	99.9 %	98.9%	0.1	193.6

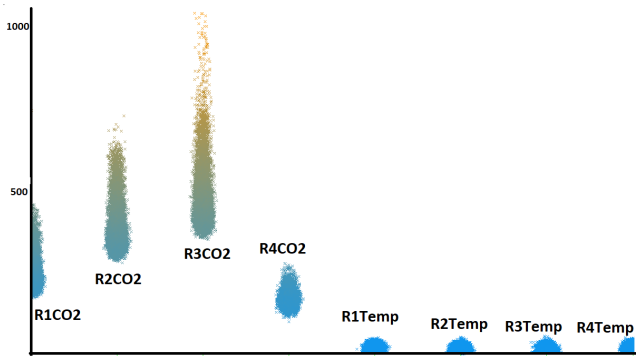


FIGURE 3. instance distribution by sensor.

[43], [45], [46], Ensemble-DNN [44], Support Vector Machine based Dimensionality Reduction [47].

B. ANOMALY-BASED INTRUSION DETECTION

This part describes the implementation and evaluation carried out in order to demonstrate the feasibility and accuracy of our AI framework to detect cyber-attacks based on the analysis of anomaly behaviors (uncommon sensor data values) in IoT system. The proposed AI framework leverages the tempo-spatial correlation between different sensor data for detecting the threats. Uncommon sensorized values indicate that the IoT device reporting the values might be under attack, e.g. infected by some malware, or being impersonated a through man-inthe-middle. Concretely, our IA-based framework detects the IoT devices malfunctioning, and enforce a reaction countermeasure accordingly. Although it is out of the scope of this paper, for the sake of completeness, it is worth mentioning that our framework when deployed in the smart building testbed scenario, enforces a mitigation plan that 1) re-configures the vAAA (virtual authentication agent), 2) enables a vChannelProtection to establish secure DTLs communications, 3) enforces new traffic filtering rules with SDN to drop malicious traffic, and 4) optionally turns-off and/or flashes the IoT device. These reaction countermeasures are being implemented and evaluated in the scope of Anastacia EU project [26], [48], [49], and are beyond the scope of this paper, which focuses on evaluating the machine learning mechanisms to detect the cyber-attacks in IoT systems.

1) Data Collection: The dataset adopted in our work obtained from real sensor data of four different rooms in our smart building testbed. We observed the measurements of temperature and CO2 for each room every 2 minutes for a duration of one month. The dataset is described with the attributes (ID, Room, SensorValueCO2, SensorValue Temperature, Class (Optional)) and it contains measurements of 67876 samples considerd as normal values. We have built a model per sensor that includes co2 and temperature. Fig. 3 depicts the distribution of sensor data per room. We notice that the co2 values are different for each room on the other hand, temperatures are in the same interval in all rooms, so the same model could work for all of them. We could also use the first room for training while the others for testing.
2) datasets:
   - Single value data-set (SV): A simple data set for the generated values, it represents only the captured value and the time as features.
   - Previous five values (P5V): This approach captures the temporal correlation between the measured sensor data. Since the temperature is contextual, this data set includes context of previous values with features in different datasets from the single value data-set [date, value]. In order to keep things clear and limit criteria, we have used only the room 1 dataset. This dataset includes the 5 previous values for each value [date, value, value precedent, value 2nd precedent, value 5th precedent]. We have also noticed that there is a strong correlation between these values.
   - Previous different three values (PD3V): Similar to the previous approach, this approach leverages the time correlation between the gathered sensor data. This approach aims to prevent the repetition by considering only the last three different values each time [date, value, value different precedent, 2nd different precedent, 3rd different precedent]
   - Cross rooms: Since there is a correlation in the sensing data in all the rooms, in this approach, we have considered this correlation by combining the room values for detecting the anomalies. By leeveraging this dataset, we combine the rooms values which mght improve the accuracy, cossing the 4 rooms ends up with the data set below: [date, room 1, room 2, room 3, room 4, label].
3) One class-SVM model: In order to construct a model able to well recognize anomalies in the dataset, we target the one-class support vector machine, which was implemented and adapted using the library of python Scikit-learn. Our proposed anomaly-based IDS model

TABLE 6. Temperture training using OC-SVM results.

trining dataset/ test	split 33%	Room2
SV	99.71%	92.52%
P5V	99.71%	87.34%
PD3V	99.28%	86.51%
cross rooms	99.23%	-

TABLE 7. CO2 training using OC-SVM results.

trining dataset/ test	split 33%
SV	98.86%
P5V	99.24%
PD3V	99.13%

consists of four phases. Firstly, the dataset is preprocessed and cleaned. The second step consists of data discretization, which consists of transforming the time-series from continuous values to discrete intervals. The latest phase applies the learning algorithm gird search step is applied for classification. For the temperature dataset, we split the first room values for training and the second one for the testing. Based on the observation that there is a spatial correlation only for temperature data, we omit to test the model generated of CO2 data with another room. For this reason, we evaluate the learning models based on the detection accuracy 33% from the training dataset.

4) Results and comparison: The results obtained from temperature values show that the SV and P5V perform better than the other features combination in terms of detection accuracy where 98.86% of detection accuracy is achieved. However in the CO2 case p5V data set achieved 99.24%.

V. CONCLUDING REMARKS AND OPEN RESEARCH CHALLENGES

IoT systems are expected to revolutionize our everyday life in the near future. Among the potential value-added features, the provisioning of on-demand security measures represents a breakthrough in facing the explosion of cybersecurity attacks. In this paper, we have investigated the most common threats to IoT systems. Then, we have provided a list of promising technologies and designed a security framework to integrate them in a comprehensive way. Indeed, we strongly believe that the joint use of SDN, NFV and machine learning solutions can enable a holistic security system able to enforce the requested security policies. We have also provided a study that proves the feasibility of our AI-based security framework, which combines both, knowledge-based intrusion detection and anomaly-based intrusion detection. On one hand, regarding knowledge based detection, three different systems used for the evaluation of framework based on NSL KDD dataset:

1) System based classification algorithm,
2) Distributed attack rule-association based JRip algorithm, and,
3) Backpropagation technique, in which we performed several preprocessing techniques, such as the discretization. The obtained results are very promising, in which the evaluation metrics allowed us to well evaluate the framework and take in consideration the effect of wrongly classified attacks. On the other hand, our framework integrates an IDS for anomaly detection in sensor data adopting One-Class SVM achieved higher than 98% of detection accuracy for most of data set combinations proposed.

In the following, we describe some additional research challenges that are envisaged to be addressed by our security framework. Firstly, we are tackling the challenge of defining standardized interfaces to ease the interactions among the envisioned framework modules, including common languages to specify the IoT security policies needed to react according to the AI-based decisions. Secondly, as the IoT landscape is continuously evolving, the AI-system will need to be autonomously reconfigured in order to deal with additional emerging (and potentially unknown) IoT cyber-attacks, which do not follow previous network/systems signatures and patterns. Thirdly, another challenge deals with machine learning methods and algorithms that can be used by the reaction agent in order to dynamically planning the best countermeasure(s) to enforce according to different contexts. Finally, we also remark that ensuring a certain level of security involves additional resource consumption and potential performance degradation; therefore, the trade-off between security requirements and Quality of Service should be deeply examined within the reaction module.

REFERENCES

[1] A. Souri, A. Hussien, M. Hoseyninezhad, and M. Norouzi, "A systematic review of IoT communication strategies for an efficient smart environment," *Trans. Emerg. Telecommun. Technol.*, Aug. 2019. Art. no. e3736. [Online]. Available: https://onlinelibrary.wiley.com/action/showCitFormats?doi=10.1002%2Fett.3736

[2] T. Taleb, "Toward carrier cloud: Potential, challenges, and solutions," *IEEE Wireless Commun.*, vol. 21, no. 3, pp. 80–91, Jun. 2014.

[3] S. Lal, T. Taleb, and A. Dutta, "NFV: Security threats and best practices," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 211–217, Aug. 2017.

[4] V. Varadharajan and U. Tupakula, "Security as a service model for cloud environment," *IEEE Trans. Netw. Service Manage.*, vol. 11, no. 1, pp. 60–75, Mar. 2014.

[5] Y. Khettab, M. Bagaa, D. L. C. Dutra, T. Taleb, and N. Toumi, "Virtual security as a service for 5G verticals," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018, pp. 1–6.

[6] X. Wang, C. Wang, X. Li, V. C. M. Leung, and T. Taleb, "Federated deep reinforcement learning for Internet of Things with decentralized cooperative edge caching," *IEEE Internet Things J.*, early access, Apr. 9, 2020, doi: 10.1109/JIOT.2020.2986803.

[7] *Zero-Touch Network and Service Management (ZSM); Reference Architecture*, Standard ETSI GS ZSM 002, V1.1.1, Aug. 2019.

[8] J. Pacheco and S. Hariri, "IoT security framework for smart cyber infrastructures," in *Proc. IEEE 1st Int. Workshops Found. Appl. Self* Syst. (FAS*W)*, Sep. 2016, pp. 242–247.

[9] K. S. Sahoo, B. Sahoo, and A. Panda, "A secured SDN framework for IoT," in *Proc. Int. Conf. Man Mach. Interfacing (MAMI)*, Dec. 2015, pp. 1–4.

[10] C. Gonzalez, S. M. Charfadine, O. Flauzac, and F. Nolot, "SDN-based security framework for the IoT in distributed grid," in *Proc. Int. Multidisciplinary Conf. Comput. Energy Sci. (SpliTech)*, Jul. 2016, pp. 1–5.

[11] A. Boudi, I. Farris, M. Bagaa, and T. Taleb, "Assessing lightweight virtualization for security-as-a-service at the network edge," *IEICE Trans. Commun.*, vol. E102.B, no. 5, pp. 970–977, 2019.
[12] R. Morabito, V. Cozzolino, A. Y. Ding, N. Beijar, and J. Ott, "Consolidate IoT edge computing with lightweight virtualization," *IEEE Netw.*, vol. 32, no. 1, pp. 102–111, Jan. 2018.
[13] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches," *Peer-to-Peer Netw. Appl.*, vol. 12, no. 2, pp. 493–501, Mar. 2019.
[14] S. Zafar, S. Jangsher, O. Bouachir, M. Aloqaily, and J. B. Othman, "QoS enhancement with deep learning-based interference prediction in mobile IoT," *Comput. Commun.*, vol. 148, pp. 86–97, Dec. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366419306620
[15] L. Tseng, L. Wong, S. Otoum, M. Aloqaily, and J. B. Othman, "Blockchain for managing heterogeneous Internet of Things: A perspective architecture," *IEEE Netw.*, vol. 34, no. 1, pp. 16–23, Jan. 2020.
[16] I. Al Ridhawi, S. Otoum, M. Aloqaily, Y. Jararweh, and T. Baker, "Providing secure and reliable communication for next generation networks in smart cities," *Sustain. Cities Soc.*, vol. 56, May 2020, Art. no. 102080. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2210670720300676
[17] J. Canedo and A. Skjellum, "Using machine learning to secure IoT systems," in *Proc. 14th Annu. Conf. Privacy, Secur. Trust (PST)*, Dec. 2016, pp. 219–222.
[18] X. Wang, Y. Han, V. C. M. Leung, D. Niyato, X. Yan, and X. Chen, "Convergence of edge computing and deep learning: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, early access, Jan. 30, 2020, doi: 10.1109/COMST.2020.2970550.
[19] M. Aloqaily, S. Otoum, I. A. Ridhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," *Ad Hoc Netw.*, vol. 90, Jul. 2019, Art. no. 101842. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870519301131
[20] A. Molina Zarca, J. B. Bernabe, R. Trapero, D. Rivera, J. Villalobos, A. Skarmeta, S. Bianchi, A. Zafeiropoulos, and P. Gouvas, "Security management architecture for NFV/SDN-aware IoT systems," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8005–8020, Oct. 2019.
[21] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, p. 15, 2009.
[22] B. B. Zarpelão, R. S Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl.*, vol. 84, pp. 25–37, Apr. 2017.
[23] A. Molina Zarca, J. Bernal Bernabe, I. Farris, Y. Khettab, T. Taleb, and A. Skarmeta, "Enhancing IoT security through network softwarization and virtual security appliances," *Int. J. Netw. Manage.*, vol. 28, no. 5, Sep. 2018, Art. no. e2038.
[24] S. Lal, A. Kalliola, I. Oliver, K. Ahola, and T. Taleb, "Securing VNF communication in NFVI," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Sep. 2017, pp. 187–192.
[25] S. Lal, S. Ravidas, I. Oliver, and T. Taleb, "Assuring virtual network function image integrity and host sealing in telco cloue," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.
[26] I. Farris, J. B. Bernabe, N. Toumi, D. Garcia-Carrillo, T. Taleb, A. Skarmeta, and B. Sahlin, "Towards provisioning of SDN/NFV-based security enablers for integrated protection of IoT systems," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Sep. 2017, pp. 169–174.
[27] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1153–1176, 2nd Quart., 2016.
[28] J. W. Branch, C. Giannella, B. Szymanski, R. Wolff, and H. Kargupta, "In-network outlier detection in wireless sensor networks," *Knowl. Inf. Syst.*, vol. 34, no. 1, pp. 23–54, Jan. 2013.
[29] R. Lippmann, J. W. Haines, D. J. Fried, J. Korba, and K. Das, "The 1999 DARPA off-line intrusion detection evaluation," *Comput. Netw.*, vol. 34, no. 4, pp. 579–595, Oct. 2000.
[30] U. Fayyad, K. Shim, P. Bradley, and S. Sarawagi, *ACM SIGKDD Explorations Newsletter*, vol. 2, no. 2. New York, NY, USA: Association for Computing Machinery, 2000.
[31] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," *Comput. Secur.*, vol. 31, no. 3, pp. 357–374, May 2012.
[32] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl.*, Jul. 2009, pp. 1–6.
[33] M. Hacibeyoğlu and M. H. Ibrahim, "Comparison of the effect of unsupervised and supervised discretization methods on classification process," *Int. J. Intell. Syst. Appl. Eng.*, vol. 4, no. 1, pp. 105–108, Dec. 2016.
[34] J. Han, J. Pei, and M. Kamber, *Data Mining: Concepts and Techniques*. Amsterdam, The Netherlands: Elsevier, 2011.
[35] G. Gu, P. Fogla, D. Dagon, W. Lee, and B. Skorić, "Measuring intrusion detection capability: An information-theoretic approach," in *Proc. ACM Symp. Inf., Comput. Commun. Secur. (ASIACCS)*. New York, NY, USA: ACM, 2006, pp. 90–101.
[36] C. Elkan, "Results of the KDD'99 classifier learning," *ACM SIGKDD Explor. Newslett.*, vol. 1, no. 2, pp. 63–64, 2000.
[37] P. Akshaya, "Intrusion detection system using machine learning approach," *Int. J. Eng. Comput. Sci.*, vol. 5, no. 10, Oct. 2016.
[38] M. A. Ambusaidi, X. He, P. Nanda, and Z. Tan, "Building an intrusion detection system using a filter-based feature selection algorithm," *IEEE Trans. Comput.*, vol. 65, no. 10, pp. 2986–2998, Oct. 2016.
[39] N. Moustafa, G. Creech, and J. Slay, "Big data analytics for intrusion detection system: Statistical decision-making using finite Dirichlet mixture models," in *Data Analytics and Decision Support for Cybersecurity*. Springer, 2017, pp. 127–156.
[40] C.-F. Tsai and C.-Y. Lin, "A triangle area based nearest neighbors approach to intrusion detection," *Pattern Recognit.*, vol. 43, no. 1, pp. 222–229, Jan. 2010.
[41] M. Z. Alom, V. Bontupalli, and T. M. Taha, "Intrusion detection using deep belief networks," in *Proc. Nat. Aerosp. Electron. Conf. (NAECON)*, Jun. 2015, pp. 339–344.
[42] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.
[43] 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 *Proc. Int. Conf. Wireless Netw. Mobile Commun. (WINCOM)*, Oct. 2016, pp. 258–263.
[44] S. A. Ludwig, "Intrusion detection of multiple attack classes using a deep neural net ensemble," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Nov. 2017, pp. 1–7.
[45] M. AL-Hawawreh, N. Moustafa, and E. Sitnikova, "Identification of malicious activities in industrial Internet of Things based on deep learning models," *J. Inf. Secur. Appl.*, vol. 41, pp. 1–11, Aug. 2018.
[46] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 2, no. 1, pp. 41–50, Feb. 2018.
[47] B. Subba, S. Biswas, and S. Karmakar, "Enhancing performance of anomaly based intrusion detection systems through dimensionality reduction using principal component analysis," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Nov. 2016, pp. 1–6.
[48] A. M. Zarca, D. Garcia-Carrillo, J. B. Bernabe, J. Ortiz, R. Marin-Perez, and A. Skarmeta, "Managing AAA in NFV/SDN-enabled IoT scenarios," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2018, pp. 1–7.
[49] A. M. Zarca, J. B. Bernabe, A. Skarmeta, and J. M. A. Calero, "Virtual IoT HoneyNets to mitigate cyberattacks in SDN/NFV-enabled IoT networks," *IEEE J. Sel. Areas Commun.*, early access, Apr. 8, 2020, doi: 10.1109/JSAC.2020.2986621.

MILOUD BAGAA (Member, IEEE) received the Engineering, master's, and Ph.D. degrees from the University of Science and Technology Houari Boumediene, Algiers, Algeria, in 2005, 2008, and 2014, respectively. From 2009 to 2015, he was a Researcher with the Research Center on Scientific and Technical Information, Algiers. From 2015 to 2016, he was with the Norwegian University of Science and Technology, Trondheim, Norway. He is currently a Senior Researcher with Aalto University. His research interests include wireless sensor networks, the Internet of Things, 5G wireless communication, security, and networking modeling. From 2015 to 2016, he received the Postdoctoral Fellowship from the European Research Consortium for Informatics and Mathematics.

TARIK TALEB (Senior Member, IEEE) received the B.E. degree (Hons.) in information engineering and the M.Sc. and Ph.D. degrees in information sciences from GSIS, Tohoku University, Sendai, Japan, in 2001, 2003, and 2005, respectively. He is currently a Professor with the School of Electrical Engineering, Aalto University, Espoo, Finland. He is a member of the IEEE Communications Society Standardization Program Development Board. In an attempt to bridge the gap between academia and industry, he founded the IEEE-Workshop on Telecommunications Standards: From Research to Standards, a successful event that was recognized with the Best Workshop Award by the IEEE Communication Society (ComSoC). Based on the success of this workshop, he has also founded and has been the Steering Committee Chair of the IEEE Conference on Standards for Communications and Networking. He is the General Chair of the 2019 edition of the IEEE Wireless Communications and Networking Conference to be held in Marrakech, Morocco. He is/was on the Editorial Board of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the *IEEE Wireless Communications Magazine, the IEEE* Journal on Internet of Things, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE Communications Surveys and Tutorials, and a number of Wiley Journals. He is the IEEE Communications Society (ComSoc) Distinguished Lecturer.

JORGE BERNAL BERNABE received the M.Sc., master's and Ph.D. degrees in computer science from the University of Murcia. He is currently a Postdoctoral Researcher with the University of Murcia. He has published over 50 articles in international conferences and journals. He has been involved in the scientific committee of numerous conferences and served as a reviewer for multiple journals. During the last years, he has been working in several European research projects such as DESEREC, Semiramis, Inter-Trust, SocIoTal, ARIES, OLYMPUS, ANASTACIA, and CyberSec4Europe. His scientific activity is mainly devoted to the security, trust and privacy management in distributed systems, and the IoT.

ANTONIO SKARMETA (Member, IEEE) received the B.S. (Hons.) in computer science from the University of Murcia, Spain, the M.S. degree in computer science from the University of Granada, and the Ph.D. degree in computer science from the University of Murcia. Since 2009, he has been a Full Professor with the Computer Science Department, University of Murcia. He has worked on different research projects in the national and international area in the networking, security, and the IoT area, like Euro6IX, ENABLE, DAIDALOS, SWIFT, SEMIRAMIS, SMARTIE, SOCIOTAL, IoT6 ANASTACIA, and CyberSec4Europe. His main interests are in the integration of security services, identity, the IoT and smart cities. He has been head of the research group ANTS since its creation in 1995. He has published over 200 international articles and being member of several program committees.