Computer Networks 151 (2019) 147–157

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Internet of Things: A survey on machine learning-based intrusion detection approaches

Kelton A.P. da Costa[a], João P. Papa[a], Celso O. Lisboa[a], Roberto Munoz[b], Victor Hugo C. de Albuquerque[c,*]

[a] Department of Computing, São Paulo State University, Bauru, Brazil
[b] School of Informatics Engineering, Universidad de Valparaíso, Valparaíso, Chile
[c] Graduate Program in Applied Informatics, University of Fortaleza, Fortaleza, CE, Brazil

ARTICLE INFO

Article history:
Received 6 September 2018
Revised 19 December 2018
Accepted 25 January 2019
Available online 28 January 2019

Keywords:
Security networks
Machine learning
Internet-of-Things
Survey
Intelligent techniques
Machine learning

ABSTRACT

In the world scenario, concerns with security and privacy regarding computer networks are always increasing. Computer security has become a necessity due to the proliferation of information technologies in everyday life. The increase in the number of Internet accesses and the emergence of new technologies, such as the Internet of Things (IoT paradigm, are accompanied by new and modern attempts to invade computer systems and networks. Companies are increasingly investing in studies to optimize the detection of these attacks. Institutions are selecting intelligent techniques to test and verify by comparing the best rates of accuracy. This research, therefore, focuses on rigorous state-of-the-art literature on Machine Learning Techniques applied in Internet-of-Things and Intrusion Detection for computer network security. The work aims, therefore, recent and in-depth research of relevant works that deal with several intelligent techniques and their applied intrusion detection architectures in computer networks with emphasis on the Internet of Things and machine learning. More than 95 works on the subject were surveyed, spanning across different themes related to security issues in IoT environments.

1. Introduction

Network security is a real necessity with the massive use of the Internet. High access to information has given rise to critical threats, ranging from a virus to a network intrusion causing significant business losses and, as a consequence, companies are investing in research using intelligent techniques to improve security as intrusion detection tools [1–5].

Updating research in the area of intrusion detection in computer networks is becoming indispensable. A major concern arises with the IP protocol implementation in version 6 (IPv6) when it comes to security in networks, and more precisely in detecting intrusions since that with the IPv6 protocol, there is a connection to the Internet of Things (IoT). Such a synergy between IPv6 and the IoT paradigm allows free access to the Internet by different devices, such as a blender, microwave, clothing, wearable devices, and cognitive buildings [6–10], among others, making network security a current challenge, where the search for intrusion detection methods for the IoT becomes fundamental.

Many works are being carried out in this context to find the best parameters and results for the detection of intrusion in IoT-based environments [11,12]. Some recent studies are addressed in this survey, such as the work of Ahmed [13], which shows that detection is an important task and that it detects anomalous data from a given data set. The author points out that intrusion detection is an interesting area and that it has been extensively studied in statistics and machine learning. Costa et al. [14] also highlighted the importance of using intelligent tools to assist intrusion detection but in the context of computer networks. In their work, the authors employed the unsupervised Optimum-Path Forest (OPF) classifier [15] for intrusion detection in computer networks. The authors proposed a nature-based approach to estimate the probability density function (pdf) used for clustering purposes, which strongly influences the quality of the classification process. Regarding the OPF classifier, Pereira et al. [16] proposed a similar approach to the one presented by Costa et al. [14] but in the context of supervised intrusion detection [17–19].

With the growth of the IoT paradigm in computer networks and the increasing use of devices for this purpose [20], concerns

* Corresponding author.
E-mail addresses: kelton@fc.unesp.br (K.A.P. da Costa), joao.papa@unesp.br (J.P. Papa), celso.lisboa@yahoo.com.br (C.O. Lisboa), roberto.munoz@uv.cl (R. Munoz), victor.albuquerque@unifor.br (V.H.C. de Albuquerque).

https://doi.org/10.1016/j.comnet.2019.01.023
1389-1286/

about connected devices on an untrustworthy Internet become inevitable [21]. Furthermore, security-related research in IoT is a promising and needed area, resulting in several techniques applied in this context to ensure, in some way, that some equipment and devices can prove to be reliable [22]. The work developed by Evans [23] presents an interesting chart that approaches the perspective of users with some IoT devices; its shown that growth is exponential.

Cyber attacks, such as man-in-the-middle (MITM) and distributed denial of service (DDoS), are also common threats to IoT. Work is being conducted to implement a system to protect an IoT against such attacks. The FOCUS [22] system uses a virtual private network (VPN) as security for IoT devices. Also, the same system sends alerts during possible DDoS attacks in IoT platforms. The study demonstrated a proof of concept and conducted experiments to evaluate performance. Results showed effectiveness to filter malicious attacks with low response time and little use of network bandwidth.

Bostani and Sheikhan [24] report that the insecurity of the Internet and wireless sensor networks, which are the main components of IoT, make the IoT vulnerable to different attacks. The same authors propose a new structure of real-time intrusion detection, which consists of anomaly-based intrusion detection modules and specifications for detecting two routing attacks known in IoT as collectors and selective routing attacks. For such purpose, the specification-based intrusion detection agents, located at the router nodes, analyze the behavior of their host nodes and send their local results to the root node through regular data packets and to an anomaly-based intrusion, which is located at the root node. It then employs the unsupervised OPF classifier to design clustering models using received data packets. The results of the experiments showed that the proposed real-time hybrid approach achieved a true positive rate of 76.19% and a false positive rate of 5.92% when collector and selective attack were launched simultaneously.

Another recent survey by Alvarenga et al. [25] discusses the issues to security, specifically regarding IoT, and the integration of real-world devices with the Internet since cybersecurity threats are brought to most daily activities. Attacks against critical infrastructures, such as power plants and public transit, can have severe consequences for cities and entire countries. The authors presented a study about intrusion detection systems methods for IoT, and they also proposed a taxonomy to classify the papers used in this research, which was based on the attributes, detection method, Intrusion Detection System (IDS) placement strategy, security threat, and validation strategy. It was also noted that the research of IDS schemes for IoT is still incipient and that the proposed solutions do not cover a wide range of attacks and IoT technologies.

Yang et al. [26] presented a study stating that IoT is designed as a network consisting of small devices distributed over a wide area. To address the limitation of existing research, an anomaly-detection-based scheme was proposed to protect the security of data aggregation from false data injection (FDI) attacks using the techniques of state estimation and sequential hypothesis testing. The main idea behind the work was to take advantage of the highly spatial-temporal correlation between consecutive observations in IoT environmental surveillance to predict future observations on the previous comments. The authors evaluated the security properties of the proposed scheme through a game-theoretical analysis. The results show that the proposed approach achieves robust capacity to detect a compromised aggregator, even if the aggregator launches an FDI attack with a very low frequency and intensity.

Neisse et al. [27] raised some concerns about intrusion vulnerabilities in IoT devices. The work proposed a Model-based Security Toolkit, which is integrated into a management framework for IoT devices and supports specification and efficient evaluation of security policies to enable the protection of user data. The paper presented a Model-based Security Toolkit integrated into the framework that allows user control and protection of user data. The work was applied in a smart city scenario to evaluate its feasibility and performance. The proposed model allowed the specification of different types of trust relationships and aspects to govern interactions among devices in IoT-based environments. Such a model considers a reference system to define the trust aspects, and it supports the design of expressive trust-based security policy rules.

Still, with respect to the security concerns in IoT, in the search to detect possible intrusions or vulnerabilities, another work, developed by Airehrour et al. [28] also expressed interest in exploring the IoT routing protocols and their weaknesses to attacks. To our best knowledge, this work was one of the first of its kind that intended to provide a broad overview of different research findings and proposed solutions concerning the issue of secure routing protocols among IoT devices.

The primary purpose of this work is to compile recent works that are oriented to improve IoT security. It also presents some research that highlight concerns about possible intrusions or anomalies, giving, therefore, proposals to cope with such issues using machine learning techniques.

The remaining of this work is organized as follows. Section 2 considers research works that make use of new and traditional machine-learning based algorithms in studies related to IoT, and it discusses relevant contributions of the literature associated with IoT security methods. Section 3 presents some widely used datasets as well as the protocols adopted in the proposed experiments. Section 4 presents the discussion and take-home message learned from the works considered in this survey. Finally, Section 5 states conclusions and a discussion about the future possibilities for research in IoT security.

1.1. Motivation

Recently, several works related to IoT have received attention in the academic area and also within the industry due to its potential use in several human activities. IoT represents a potential solution to improve the quality of life of people (e.g., the smartwatch, which monitors health through its sensors [29]), and several technologies have become popular with the fall in the sensor prices, the popularization of remote storage services, and big data.

It is apparent that the easy access to such resources strengthens IoT when devices with different resources are connected to a network, thus contributing to the emergence of new applications. Such a brand new whole ground has come with a price: the need for security. Furthermore, a concern arises regarding the level of confidence regarding the data obtained from IoT devices, and how or where this data can be used is one of our motivations for such research [30–36].

However, we realize that no work has presented an in-depth view of the application of machine learning in the context of IoT with a focus on the detection of intrusions to date, which ends up being the main contribution of this survey.

1.2. Goals

In this paper, we want to provide an overview of the research progress in security-related issues in IoT environments. The scope of this review discusses some methods based on machine learning and evolutionary computation, among others. The idea of this review is to provide information on the current literature as well to be a new source for researchers interested in IoT and security issues.

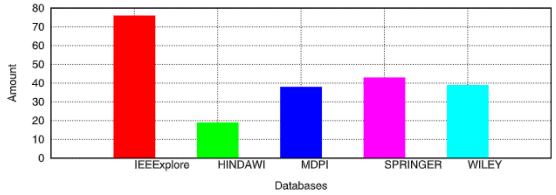


Fig. 1. Histogram of works considered in this survey.

Additionally, we also provided a clear vision of the possible challenges of existing research and highlighted the new research guidelines.

1.3. Work selection criteria

The databases considered in the search and selection of works were the IEEE Xplore, Science Direct, Springer, Hindawi Publishing Corporation, MDPI Publisher of Open Access Journals, and Wiley Online Library, mainly. The selected studies were published from 2015 until the middle of 2017, with some works published in 2018. We believe that this survey is of significant contribution to researchers and professionals in the area of security in networks and other related fields. Fig. 1 depicts the number of works found on each database and considered in this work.

2. Related works

In this section, we review works that make use of new and traditional machine learning-based algorithms to handle security issues in IoT environments. The process of compiling the works considered in this survey adopted the so-called "Systematic Literature Review" (SLR). Through SLR methodology, works can be identified, evaluated, and interpreted meaningfully. The process should be conducted in a transparent and replicable way as much as possible [37].

Conti et al. [38] published an interesting survey, which addresses the challenges and opportunities in the IoT domain. The authors portray the priority of a successful IoT network that is capable of detecting compromised nodes along with collecting and preserving evidence of an attack or malicious activity. The study focused mainly on portraying significant challenges in IoT. The authors also stated that detecting the presence of IoT systems is a challenge, considering that devices are designed to function passively and autonomously.

In the past years, using machine learning to aid security and detection in IoT environments has become extremely important to face the challenges reported previously [39,40]. However, we have not found too many works that employed machine learning in the context of security challenges in IoT-based environments.

Deep learning has also attracted considerable attention in the past years. Currently, it is recognized as a relevant approach to intrusion detection in networks in addition to acting in pattern recognition, image processing, and text mining.

Diro and Chilamkurti [41] approached deep learning as a novel intrusion detection technique for the IoT context with promising results. The authors also reported that thousands of zero-day attacks appear because of the addition of various protocols, mainly from IoT and that most of them are small variants of previously known cyber-attacks. Such a situation indicated that even advanced mechanisms such as traditional machine-learning systems face the difficulty of detecting these small mutants of attacks over time.

Ramos et al. [42] presented a survey that focused on model-based quantitative security metrics that aim to quantify overall network resilience against attacks. In this survey, an in-depth literature review of the state-of-the-art of Network Security Metrics (NSMs) has been presented focused in the Common Vulnerability Scoring System (CVSS) framework, which is used as input by several security metric models. The differences between the security metrics field and other correlate areas have also been conducted. This study carried out a comprehensive and detailed review of the main metric proposals and has been presented more specifically in the realm of model-based quantitative NSMs; a complete and thorough review of the main metric proposals has also been presented. The main pros and cons of each reviewed work have also been described. Eventually, an in-depth investigation of the main properties of the reviewed security metrics has been presented, along with open issues and suggestions for future research directions, followed by a discussion on past related work. According to what has been presented in this review, it is reasonable to assume that the field of model-based quantitative NSMs is still in development and significant more progress still needs to be done.

Granjal et al. [43] added that security metrics of such type would also be valuable for users of other Internet infrastructures, such as cloud computing and, especially, IoT, whose security has received increasing attention.

Al-Fuqaha et al. [44] surveyed some challenges and issues that belong to the design and deployment of IoT implementations, as well as the interplay between the IoT, big data analytics, cloud, and fog computing. The work presented a new intelligent technique for autonomous management, data aggregation, and protocol adaptation services to achieve better horizontal integration among IoT services. They directed on the IoT protocols and standards reviewing the different protocols and patterns in the different layers of an IoT environment and approached the main functionality and purpose of these protocols. The authors also researched the consequence of IoT, which are Big Data, cloud and fog computing, and the need for a new generation of data analytics algorithms and tools that are suitable for IoT big data, such as to be able to shrink input size. Finally, three use-cases were presented that illustrate how the different protocols presented in this survey fit together to deliver new smart IoT services that deliver new functionality to the users.

Lopez-Martin et al. [45] proposed a new network intrusion detection method specifically developed for an IoT network. The proposed method is based on a Conditional Variational Autoencoder (CVAE) with a specific architecture that integrates the intrusion labels inside the decoder layers. The proposed model is also able to perform feature reconstruction, and it also can be used in the current Network Intrusion Detection System, which is part of network monitoring systems, and particularly in IoT networks. The proposed approach operates in a single training step, therefore saving computational resources.

Fu et al. [46] argued that IoT will be a future part of 5G networks, but unfortunately, the resources of IoT as devices are constrained, and many security mechanisms are hard to implement because the safety of IoT will certainly be related to many important scenarios of the future 5G. In this work, an approach based on the automata theory was proposed concerning the vast heterogeneous IoT networks. The method uses an extension of Labelled Transition Systems to propose a uniform description of IoT systems that can detect the intrusions by comparing actions flows.

The research designed the intrusion detection approach, built the Event Databases, and implemented the Event Analyzer to achieve the IDS approaches. The proposed IDS was able to detect three types of IoT attacks: jam-attack, false-attack, and reply-attack.

Still, regarding the concern with security and prevention of intrusions in IoT, we noticed that its architecture is not yet standardized. For Adat et al. [12], organizations such as IEEE and ITU are

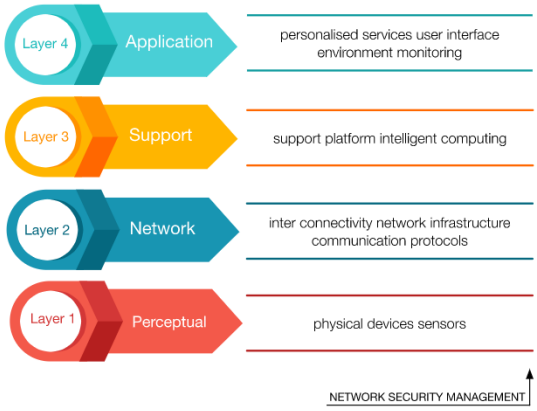


Fig. 2. A generic IoT architecture.

working on the standardization of IoT. However, some technologies such as IPv6, 6LoWPAN, IEEE 802.15.4 are then defined as a platform for IoT, yet the authors say that there are a few architectures for IoT and most of them are based on a network layer and a layer that addresses the needs of IoT. The most generic architecture proposed for IoT is depicted in Fig. 2.

Gunupudi et al. [47] showed that privacy preservation and intrusion detection is implicitly challenging and is much more complex in the context of IoT. In this work, a membership function was proposed to cluster attributes of the global dataset incrementally, being the goal to represent each high dimensional sample in the global dataset by an equivalent method with reduced dimensions. A reduced representation was obtained using a dimensionality reduction approach which is used as input for classifiers.

Flauzac et al. [48] discussed security architectures for IoT based on software-defined networking (SDN). In this context, the SDN-based architecture works with or without infrastructure, called SDN-Domain. The work described the operation of the proposed architecture and summarized the opportunity to achieve network security more efficiently and flexibly with SDN. In this paper, the network access control and global traffic monitoring for ad-hoc networks were considered, as well as the work pointed out some architectural design choices for SDN using OpenFlow and discussed their performance implications.

Wang et al. [4] emphasized that high-quality training data is important to improve detection performance. The authors proposed an effective intrusion detection framework based on Support Vector Machines (SVM) with augmented features. They implemented a logarithm marginal density ratio transformation with the goal of obtaining new and better-quality SVM detection, and their empirical results showed effective values such as good performance, high detection rate, and low false positive alarm.

López-Benítez et al. [49] focused the research on multidisciplinary solutions through a suitable platform that takes into account potential mutual effects and interactions among the different dimensions of future IoT systems. The project, called “Internet of Surprise: Self-Organising Data”, constituted a platform to obtain an accurate and realistic evaluation of IoT solutions. The prototype enables the assessment and optimization of multidisciplinary aspects of IoT systems, including issues related to hardware design, communications, and data processing.

Sedjelmaci et al. [50] employed the Nash equilibrium as a proposal for a lightweight anomaly detection technique based on the concept of game theory. The method mainly predicted the equilibrium state that allows the IDS to activate its anomaly detection mode to detect new attack signatures. The results showed that the data generated is viable, obtaining excellent detection rates, low false positive alarm, and low energy consumption. The authors used TOSSIM, a simulator of TinyOS sensor nodes [51], for experimental purposes.

Cruz et al. [52] addressed the need for an IoT middleware since resources are restricted in the majority of the devices. With such an improvement in hands, intelligent-based decision-making mechanisms could be processed in such middleware.

The research completed by Bellagente et al. [53] focused on the impact of IoT in the industrial automation world. The paper proposed a new architecture that enables the integration of currently available, legacy, industry-grade devices to be used across the Internet.

One can notice the accelerated growth of IoT caused concerns both in the convergence of the existing technologies as well as the application of new techniques and especially with respect to security. As a consequence, many relevant types of research in IoT have emerged with an emphasis specifically in IoT-based behavior when it comes to computer network security.

Several works related IoT presented new technologies that work together with the paradigm, always with an emphasis on the concern for security issues [54–59].

For the sake of clarification, Tables 1 and 2 summarized the works by the main purpose of the paper (PU), communication protocol (CP), application protocols (AP), data format (DF), machine learning technique (MLT), and precision rate (PR).

3. Methods and datasets

In this section, we present some widely used datasets and methodology employed in papers related to IoT and its security issues [2,5,60–67].

Diro and Chilamkurti [41] employed three original-size datasets known as KDDCUP99, ISCX, and NSL-KDD for experimental purposes regarding intrusion detection in computer networks. They proposed a distributed deep learning-based IoT/fog network attack detection system, and the experiments showed the successful adoption of artificial intelligence to cybersecurity purposes. The authors also designed and implemented the system for attack detection in a distributed architecture concerning IoT applications, such as smart cities. The evaluation process has considered accuracy, detection rate, and false alarm rate as performance metrics to show the effectiveness of deep models over shallow models. In the first round of experiments, the 2-class (normal and attack) and 4-class (normal, DoS, Probe, R2L.U2R) categories were considered in the experimental section. Besides, unseen test data were chosen to represent zero-day attack detections.

The study comprised two main objectives. The first one aimed to compare the results of the distributed attack detection with a centralized system conducted through deploying the deep learning model on a single node for the centralized system and multiple coordinated nodes for distributed attack detection. To test the performance of the parallelism, the number of machines used for training the network as a function of training accuracy were varied. The second goal was to evaluate the effectiveness of deep learning against shallow learning algorithms for attack detection in IoT-based systems. The deep learning system, after hyper-parameter optimization, has used 123 input features, 150 neurons for the first layer, 120 and 50 neurons for the second and third layers, respectively, and the last layer contains a number of neurons equal to the number of classes. The model used batches of different sizes and 50 epochs, and it has been trained with dropout to avoid the overfitting problem.

A recent work developed by Acharjya et al. [68] presented a method that detects specific activities, such as the dropping of people based on resources, called Motion Projection Profile. The temporal difference is extracted from the image so that it is possible to represent several postural levels of a person. Such drops

Table 1
IoT summarized works - Part 1.

Reference	PU	CP	AP	DF	MLT	PR
[1]	This work, in order to detect network attacks, using k-means algorithm a new semi-supervised anomaly detection system has been designed and implemented.	TCP/IP	–	–	k-means	80.19%
[2]	A useful intrusion detection framework by adopting a new optimization method, specifically, time-varying chaos particle swarm optimization.	–	–	–	SVM, MCLPDR	97.23%
[3]	An intrusion detection technique that considers various points like the hugeness of network traffic dataset, feature selection, low accuracy and high rate of false alarms.	TCP/IP, UDP, ICMP	–	–	OS-ELM	98.66%
[4]	A useful intrusion detection framework based on a support vector machine with augmented features.	TCP	–	–	SVM	99.18%
[5]	A build a model for intrusion detection system using random forest classifier.	–	–	–	Random Forest	99.67%
[6]	Examines the connection of Building Information Modeling and IoT for filling these issues in the management of cognitive buildings.	TCP/IP	–	neutral data format	–	–
[11]	A novel method for intrusion detection system based on sampling with Least Square Support Vector Machine (LS-SVM).	TCP/IP	–	–	LS-SVM	[99,62%–99.78%]
[12]	Explain the history, background, statistics of IoT and security-based analysis of IoT architecture	RPL, IPv6	–	–	–	–
[13]	Presents an in-depth investigation of four significant categories of anomaly detection techniques which involve classification, statistical, information theory and clustering.	TCP/IP	–	–	SVM	–
[14]	A nature-inspired approach to estimate the probability density function used for data clustering based on the Optimum-Path Forest algorithm (OPF).	–	–	–	Optimum-path forest, Bat algorithm, Firefly Algorithm	–
[20]	An overview of the major challenges facing IoTs. (Security, privacy, and interoperability)	TCP/IP, 6loW-PAN, RPL	CoAP	–	–	–
[21]	A real-world simulation service uses Internet of Things capable objects to detect behavioral-based anomalies within a simulated smart home/vicinity	IP	–	–	–	–
[22]	A FoG Computing based Security system to protect the IoT against malware cyber attacks.	MQTT, IP	TLS, SSL	–	–	–
[23]	Educate you in plain and simple terms so you can be well versed in IoT and understand its potential to change everything we know to be true today.	–	–	–	–	
[24]	A novel real-time hybrid intrusion detection frame- work	6LoWPAN, RPL	CoAP, DTLS	–	Optimum-Path Forest Clustering, SA-IDSs	96.02%
[25]	A survey of IDS's research efforts for IoT. In order to identify the main trends, open questions and future research possibilities.	6LoWPAN, RPL	CoAP	–	–	–
[26]	Using DDF-based state estimation techniques to detect false aggregate data and determine nodes that are suspected of injecting false data using the SHT.	CSMA/CA	–	–	–	–
[27]	A Modelbased Security Toolkit, which is integrated in a management framework for IoT devices, and supports specification and efficient evaluation of security policies to enable the protection of user data.	–	LWM2M	–	–	–
[28]	A propose the Internet of Things and its significance as well as growing trends in today's global IT scenario. A survey of the threats correlated with IoT routing and identifies few of the research challenges as discussed by the research fraternity and some of the potential research directions in achieving secure and sustainable routing with IoT devices.	LLN, IPV6, 6LoW-PAN, RPL	CoAP, DTLS	–	–	–
[37]	To propose extensive guidelines for systematic literature reviews relevant for software engineering researchers, including Ph.D. students.	–	–	–	–	–
[38]	Introduce existing significant security and forensics challenges within the IoT domain and then briefly discuss papers published in this special issue targeting recognized challenges.	–	–	–	–	–
[39]	To analyze different supervised algorithms for the anomaly-based detection techniques.	IP	–	–	SVM, Naive Bayes, J48	–

are detected by analyzing the projection profiles consisting of motion pixels as each row, column, diagonal left, and diagonal right temporal image changes, thus allowing real-time recognition of the posture of the person.

Furthermore relating to intrusion detection, several works also been approaching that utilize Support Vector Machines with polynomial and Radial Basis Function (RBF) kernels, K-Nearest Neighbors (KNN), and the decision tree algorithm (J48) [69–76] being

Table 2
IoT summarized works - Part 2.

Reference	PU	CP	AP	DF	MLT	PR
[40]	Show the various facets of network anomaly detection so that a researcher can quickly become familiar with all these aspects.	TCP/IP, UDP, ICMP	-	-	ADAM, SVM, CSF-KNN, OCSVM	-
[41]	Adopt a new approach, deep learning, cyber security to enable the detection of attacks in the social Internet of Things.	TCP/IP, ICMP, UDP	Telnet, FTP, IMAP	-	SVM	-
[42]	The article presents a thorough state-of-the-art survey of model-based Network Security Metrics.	TCP/IP	HTTP, SSH, FTP, RSH	-	-	-
[43]	It analyzes existing protocols and mechanisms to protect IoT communications, as well as open research questions.	6LoPAN, RPL, UDP, IPV6	CoRE, CoAP	-	-	-
[44]	Provide an overview IoT, with an emphasis on enabling technologies, protocols, and application issues.	RPL, 6LoWPAN, IPV4/IPV6	DDS, CoAP, AMQP, MQTT, MQTT-SN, XMPP, HTTP REST	-	-	-
[45]	A new network intrusion detection method that is appropriate for an Internet of Things network.	TCP, ICMP, UDP	-	-	random forest, linear SVM, multinomial	99.00%, 92.00%, 65.00%
[46]	Analyzes the existing CRADS, GIDP, and other intrusion detection frameworks for MANET.	TCP/IP	-	-	-	-
[47]	To design a fuzzy membership function to approach both dimensionality and anomaly mining so as reduce the computational complexity and improve computational accuracies of classifier algorithms.	-	-	-	KNN, J48, SVM	-
[48]	Describes the operation of the on Big Data, Data Mining Challenges on IoT and Pervasive Systems and summarizes the opportunity to achieve network security in a more efficient and flexible with SDN.	IP	-	-	-	-
[49]	A prototype developed in the context of the EPSRC/eFutures-funded project Internet of Surprise: Self-Organising Data	TCP/IP	AMQP, CoAP, DHCP, DNS, MQTT	-	-	-
[50]	To secure low resources IoT devices such as smart meters and sensors against any malicious behaviors.	-	-	-	SVM, NNs	-
[51]	To investigate how we can explore the characteristics of the sensor network domain to achieve scale, fidelity, and integrity that would be intractable in a general purpose context.	TCP/IP	-	-	-	-
[52]	Develops on a systematic analysis of the related literature, exploring the differences between the current Internet and IoT-based systems, presenting an in-depth investigation of the challenges and future scenes on IoT middleware.	TCP/IP, UDP	HTTP, CoAP, MQTT	-	-	-
[53]	To present and discusses a set of basic requirements and a preliminary performance evaluation of a sample application.	TCP/IP	DCP	-	-	-
[54]	Proposes an architecture that employs a Bayesian event prediction model that uses historical event data generated by the IoT cloud to calculate the probability of future events.	-	-	-	-	-
[55]	To review the advances on issues of security and privacy in IoV, including security and privacy requirements, attack types, and the relevant solutions, and discuss challenges and future trends in this area.	SAODV, Ariadne, SRP	-	-	SVM	-
[56]	Proposes security measures for a defined uniform and transparent Internet of Things middleware, named UIoT.	6LowPAN, TCP/IP, UPnP	HTTP, HTTPS, TLS, CoAP	-	-	-
[57]	Propose an approach for the detection of incidents in the Internet of Things, based on a correlation analysis of the devices' information.	-	-	-	-	-

that for the classification and recognition of the types of intrusions, the SVM with RBF presented reasonable precisions.

Most of the work conducted so far takes advantage of datasets already used for other research. Basically, a lot of research proposes the use of several classifiers with several datasets and analyzes some of the requirements proposed in the study, such as accuracy, error rate, and the possibility of these results being feasible to employ in devices that consume low computational resources, including low-powered devices to be used in the IoT context [77–80].

The Electronic IT and Imaging Lab [81] created a dataset in video format that detected falls captured in a real-time environment through video surveillance using an RGB camera with a rate of 25 frames per second and resolution of 320×240 pixels. The dataset consists of two types of events: normal daily activities and actions of falls performed by various actors in different environments. Besides, 250 video sequences were captured with a time of 10 seconds each.

The video sequence contains factors to be analyzed such as illumination, occlusions, and textured background. After feature extraction, the proposed method was tested using SVM with polynomial and RBF kernels, K-NN, and a decision tree classifier using a 10-fold cross-validation approach for comparison purposes. The performance of the classifiers was obtained considering the error rate and the confusion matrix.

Another interesting work was carried out by Guo et al. [82]. The authors addressed a critical approach related to an indoor location for IoT-based applications such as tracking the company's assets, unattended parking, monitoring, geolocation, and smart cities. In short, the authors developed a framework for this context and employed the Adaboost and Random Forest classifiers. Simulations

demonstrated the robustness in performance for the internal location problem.

Recent advances show that Convolutional Neural Networks (CNNs) have an excellent performance in image classification tasks, especially when the size of the datasets is large and can also be applied to related devices in the IoT context. Shen et al. [83] applied CNN focusing on the high requirement for communication and data training that can be found in IoT architectures. Two popular datasets, MNIST and CIFAR-10, were used for training and testing. The MNIST dataset constituted 60,000 training examples and 10,000 for testing purposes. The size of each digit image is 28×28, and the CIFAR-10 dataset consists of 50,000 training examples and 10,000 for testing. The results were promising and appropriate to achieve good performance when implemented in IoT devices for management and better use of the resources offered by it.

A paper presented by Azmoodeh et al. [84] addresses the Internet of Things (IoT) for military environments, which constitutes a diverse amount of devices connected to the Internet, ranging from medical devices to wearable technologies. The aforementioned work presented a new dataset consisting of 1,078 normal samples and 128 samples with malware specifically for IoT applications based on an Advanced RISC Machines (ARM) architectures. The samples were collected using the VirusTotal3 Threat Intelligence platform from February 2015 through January 2017.

The assessments demonstrated the robustness of the approach in detecting malware with an accuracy rate of around 98% while still obtaining the ability to mitigate attacks of insertion of unwanted code. For the experiments, the authors used a detection approach based on the selection of sequence code classes as a resource for the classification of samples. A feature chart was created for each sample, and a deep learning approach was applied for malware classification purposes.

Two recent works that deal specifically with the use of machine learning techniques concerning security issues in IoT architectures over KDD99 dataset can be referred as well. Al-Yaseen et al. [85] proposed a modified K-means approach to reduce the size of the training dataset as well as to balance the data for training SVMs and Extreme Learning Machines (ELMs). According to the experiments, the performance of the proposed model achieved an accuracy of 95.75% and a false alarm rate of 1.87%.

The other work, conducted by Feng et al. [86], a new machine-learning based data classification algorithm was used and further applied to network intrusion detection. The proposed approach, named Clustering based on Self-Organized Ant Colony Network (CSOACN) was employed to classify network activities as normal or abnormal. This new approach combines the SVM method with CSOACNs to take the advantages of both techniques, and the experiments show that CSVAC (Combining Support Vectors with Ant Colony) outperforms SVM or CSOACN alone regarding both classification rate and run-time efficiency.

It can also be noted that many recent works focus mainly on the development of frameworks that can, in a way, contribute to the IoT architecture in various aspects, such as energy consumption, consumption of local bandwidth and Internet, and intrusion detection methods related to data security. The implementation of frameworks and specific environments for simulation and testing in IoT platforms can be seen in the research by Zhao et al. [87], Bako and Ismail [88], Wang and Liu [89], Wu and Wang [90], Li et al. [91] and Yan et al. [92].

For a better identification and visualization of all the datasets related to this survey, Table 3 presents the works summarized

Table 3
Databases used in the works considered in the paper.

Reference	DN	DS	CTD
[60]	KDD'99, NSL-KDD, Noisy Dataset	–	TCP-dump raw data
[61]	–	–	–
[62]	Dataset generated by personal computer	20,000 records	–
[63]	NSL-KDD, KDDCUP99	–	Symbolic data
[64]	KDD CUP 1999	212,123 samples	–
[65]	Piping dataset, Crack-box dataset	2,460, 1380	levee passive seismic data
[66]	NSL-KDD	148,517	Text file
[67]	NSL-KDD, KDDCup 1999	33,300 records	–
[93]	–	–	–
[69]	NSL-KDD	–	–
[70]	KDD	148,753 records	–
[71]	–	307,641	Text file
[72]	–	–	–
[73]	NSL-KDD Cup 1999	10,000	–
[74]	NSL-KDD	148,516	TCP packets
[75]	AWID	1,795,575	–
[76]	NSL-KDD Cup 1999	106,154	TCP, UDP and ICMP data
[77]	–	–	–
[78]	–	–	–
[79]	–	–	–
[80]	–	–	–
[81]	–	250	Video data
[82]	–	–	–
[83]	MNIST, CIFA-10	70,000, 60,000	Image data
[84]	Dataset created by the authors	1206	OpCodes
[85]	KDD Cup 1999	494,021	–
[86]	KDD99 dataset	548,015	network data
[87]	A real world smart grid dataset	–	–
[88]	–	–	–
[89]	–	–	–
[90]	–	–	–
[91]	Open dataset from Kaggle	25,000	Image data
[92]	–	–	–
Janusz Kacprzyk	Fall Detection Dataset	250	Video data
[94]	–	–	–
[95]	–	–	–
[96]	–	–	–

through the dataset name (DN) and size (DS), as well as the content type of the dataset (CTD).

4. Discussion and open issues

With the growth of IoT, concerns about data security risks increase exponentially. Due to some factors such as the vulnerabilities of devices that are used by IoT, these vulnerabilities occur through viruses, denial of service attacks, and intrusion attempts, among others. More robust measures should be taken to avoid such situations, allowing system developers and IoT devices to improve their methods for better security mitigation. It is necessary to identify all the vulnerabilities and threats that may exist that are designed explicitly for IoT architectures.

To reduce potential threats, it is perceived that the need for more studies that focus on the knowledge of threats becomes a fact for that context and that challenges in their security, such as confidentiality and privacy, have been identified and must be addressed and avoided.

There is a number of works to be developed regarding security issues in IoT-based environments, specifically for suppliers and users, to increase the reliability of IoT applications gradually. Addressing security challenges more precisely in IoT services and devices is the trend to be realized from now on.

For Perumal et al. [97], IoT is still in full development according to the increasing use of sensors for information that is collected, organized, and mined on the Web, thus including sensor-based hardware. Fig. 3 depicts three main views of IoT that clarifies such context: (i) “Things Oriented Vision” is the main point for the use of embedded sensors to trace anything; (ii) “Internet Oriented Vision”, the main point is the need to create smart objects; and (iii) “Semantic Oriented View”, the main point concerns problems with the data interpretation.

Another critical aspect addressed by Rayes and Salam [94] is that the security risks for IoT are severe if the devices are employed in companies since an attacker could have access through invasion techniques in any of these intelligent devices, allowing company espionage by the invader.

Still, the same authors present some challenges to security in IoT, such as IoT combined with multiple technologies, scalability, Big Data, the availability of services for IoT, the hardware limitation for applications, remote locations to access, mobility, and Delay-Sensitive Service.

We observed that are specific methods for detecting intrusion in the network, individually for each existing data communication technology. Besides, IoT has being refined continually through different techniques to address such intrusions.

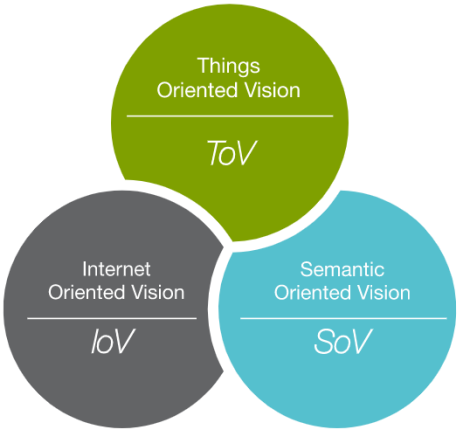


Fig. 3. The three main views of IoT.

In recent research focusing on IoT beyond the concern of power consumption [95,96], the trend will be to interact in all layers of the network architectures that are supported by IDS and not only focusing on the lowest layer level, as is usual. A trend also identified in the literature is the use of IDS tools that support IoT, a direction that should be the focus of many software manufacturers, in both open source and paid software.

5. Conclusions

This research has noticed that intrusion detection within the Internet of Things context still presents a challenge. As the Internet evolves into IoT, the focus shifts from connectivity to data. This work, therefore, focused on the newest studies in intrusion detection and intelligent techniques applied to IoT to keep data secure.

The works surveyed in this paper discussed, mainly, the concern and many efforts made by the scientific community as well as the industry focused on the development of optimized security protocols that achieve reasonable protection while maintaining a low or moderate energy consumption.

The work also presents several intelligent techniques that are applied in the context of security in computer networks, and more precisely in intrusion detection. Such techniques seek to achieve better recognition rates in intrusion detection, but it is perceived that the false positive rate is still the problem to be addressed in all studies.

Some techniques can reduce the false positive rate but, in contrast, the training time and classification increases. On the other hand, some techniques perform the inverse process, i.e., the false positive rate is stabilized, but at the price of a high computational burden for training and testing. Such an issue is way relevant for intrusion detection, where real-time detection is a relevant factor.

Acknowledgments

The authors are grateful to FAPESP grants #2017/22905-6, #2013/07375-0, #2014/12236-1, and #2016/19403-6 and by the Brazilian National Council for Research and Development (CNPq) via grants No. 429003/2018 − 8, 304315/2017 − 6, 430274/2018 − 1, 307066/2017 − 7 and 427968/2018 − 6.

References

[1] M.E. Karsligil, A.G. Yavuz, M.A. Guvensan, K. Hanifi, H. Bank, Network intrusion detection using machine learning anomaly detection algorithms, in: 25th Signal Processing and Communications Applications Conference (SIU), IEEE, 2017 [Online]. Available, doi:10.1109/siu.2017.7960616.

[2] S.M.H. Bamakan, H. Wang, T. Yingjie, Y. Shi, An effective intrusion detection framework based on mclp/svm optimized by time-varying chaos particle swarm optimization, Neurocomputing 199 (2016) 90–102. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0925231216300510.

[3] R. Singh, H. Kumar, R.K. Singla, An intrusion detection system using network traffic profiling and online sequential extreme learning machine, Expert Syst. Appl. 42 (22) (2015) 8609–8624. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0957417415004753.

[4] H. Wang, J. Gu, S. Wang, An effective intrusion detection framework based on svm with feature augmentation, Knowl. Based Syst. 136 (2017) 130–139. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S095070511730415X.

[5] N. Farnaaz, M.A. Jabbar, Random forest modeling for network intrusion detection system, Procedia Comput. Sci. 89 (Supplement C) (2016) 213–217.

[6] D. Pasini, S.M. Ventura, S. Rinaldi, P. Bellagente, A. Flammini, A.L.C. Ciribini, Exploiting internet of things and building information modeling framework for management of cognitive buildings, in: IEEE International Smart Cities Conference (ISC2), IEEE, 2016 [Online]. Available, doi:10.1109/isc2.2016.7580817.

[7] W. Wu, S. Pirbhulal, H. Zhang, S.C. Mukhopadhyay, Quantitative assessment for self-tracking of acute stress based on triangulation principle in a wearable sensor system, IEEE J. Biomed. Health Inform. (2018) 1.

[8] W. Wu, H. Zhang, S. Pirbhulal, S. Mukhopadhyay, Y. Zhang, Assessment of biofeedback training for emotion management through wearable textile physiological monitoring system, IEEE Sens. J. 15 (12) (2015) 7087–7095.

[9] W. Wu, S. Pirbhulal, K. Sangaiah, S.M. Chandra, G. Li, Optimization of signal quality over comfortability of textile electrodes for ecg monitoring in fog computing based medical applications, Future Gener. Comput. Syst. 86 (2018) 515–526.

[10] S. Pirbhulal, H. Zhang, W. Wu, S.C. Mukhopadhyay, Y. Zhang, Heartbeats based biometric random binary sequences generation to secure wireless body sensor networks, IEEE Trans. Biomed. Eng. 65 (12) (2018) 2751–2759.

[11] E. Kabir, J. Hu, H. Wang, G. Zhuo, A novel statistical technique for intrusion detection systems, Future Gener. Comput. Syst. 79 (2018) 303–318. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17301371.

[12] V. Adat, B.B. Gupta, Security in internet of things: issues, challenges, taxonomy, and architecture, Telecommun. Syst. 67 (3) (2018) 423–441.

[13] M. Ahmed, A.N. Mahmood, J. Hu, A survey of network anomaly detection techniques, J. Netw. Comput. Appl. 60 (2016) 19–31. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804515002891.

[14] K.A.P. Costa, Pereira, R.Y.M. Nakamura, C.R. Pereira, J.P. Papa, A.X. Falcão, A nature-inspired approach to speed up optimum-path forest clustering and its application to intrusion detection in computer networks, Inf. Sci. 294 (2015) 95–108. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025514009311.

[15] L.M. Rocha, F.A.M. Cappabianco, A.X. Falcão, Data clustering as an optimum–path forest problem with applications in image analysis, Int. J. Imaging Syst. Technol. 19 (2) (2009) 50–68.

[16] C.R. Pereira, R.Y.M. Nakamura, K.A.P. Costa, J.P. Papa, An optimum-path forest framework for intrusion detection in computer networks, Eng. Appl. Artif. Intell. 25 (6) (2012) 1226–1234.

[17] J.P. Papa, A.X. Falcão, C.T.N. Suzuki, Supervised pattern classification based on optimum-path forest, Int. J. Imaging Syst. Technol. 19 (2) (2009) 120–131.

[18] J.P. Papa, A.X. Falcão, V.H.C. Albuquerque, J.M.R.S. Tavares, Efficient supervised optimum-path forest classification for large datasets, Pattern Recognit. 45 (1) (2012) 512–520.

[19] J.P. Papa, G.H. Rosa, L.P. Papa, A binary-constrained geometric semantic genetic programming for feature selection purposes, Pattern Recognit. Lett. 100 (Supplement C) (2017) 59–66.

[20] F. Javed, M.K. Afzal, M. Sharif, B. Kim, Internet of things (IoTs) operating systems support, networking technologies, applications, and challenges: a comparative review, IEEE Commun. Surv. Tut. (2018) 1 [Online]. Available, doi:10.1109/comst.2018.2817685.

[21] B. Arrington, L. Barnett, R. Rufus, A. Esterline, Behavioral modeling intrusion detection system (BMIDS) using internet of things (IoT) behavior-based anomaly detection via immunity-inspired algorithms, in: 25th International Conference on Computer Communication and Networks (ICCCN), IEEE, 2016 [Online]. Available, doi:10.1109/icccn.2016.7568495.

[22] S. Alharbi, P. Rodriguez, R. Maharaja, P. Iyer, N. Bose, Z. Ye, FOCUS: a fog computing-based security system for the internet of things, in: 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), IEEE, 2018 [Online]. Available, doi:10.1109/ccnc.2018.8319238.

[23] D. Evans, The internet of things: how the next evolution of the internet is changing everything, Cisco White Paper (2011) 1–11.

[24] H. Bostani, M. Sheikhan, Hybrid of anomaly-based and specification-based ids for internet of things using unsupervised opf based on mapreduce approach, Comput. Commun. 98 (Supplement C) (2017) 52–71.

[25] B.B. Zarpelao, R.S. Miani, C.T. Kawakani, S.C. Alvarenga, A survey of intrusion detection in internet of things, J. Netw. Comput. Appl. 84 (2017) 25–37. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804517300802.

[26] L. Yang, C. Ding, M. Wu, K. Wang, Robust detection of false data injection attacks for data aggregation in an internet of things-based environmental surveillance, Comput. Networks 129 (2017) 410–428. Special Issue on 5G Wireless Networks for IoT and Body Sensors. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128617302372.

[27] R. Neisse, G. Steri, I.N. Fovino, G. Baldini, Seckit: a model-based security toolkit for the internet of things, Comput. Secur. 54 (Supplement C) (2015) 60–76.

[28] D. Airehrour, J. Gutierrez, S.K. Ray, Secure routing for internet of things: a survey, J. Netw. Comput. Appl. 66 (2016) 198–213. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804516300133.

[29] I. Romdhani, Chapter 9 - Confidentiality and security for iot based healthcare, in: S. Li, L.D. Xu (Eds.), Securing the Internet of Things, Syngress, Boston, 2017, pp. 133–139.

[30] S. Li, Chapter 1 - Introduction: Securing the internet of things, in: S. Li, L.D. Xu (Eds.), Securing the Internet of Things, Syngress, Boston, 2017, pp. 1–25.

[31] S. Li, Chapter 2 - Security architecture in the internet of things, in: S. Li, L.D. Xu (Eds.), Securing the Internet of Things, Syngress, Boston, 2017, pp. 27–48.

[32] I. Romdhani, Chapter 8 - Security concerns in social iot, in: S. Li, L.D. Xu (Eds.), Securing the Internet of Things, Syngress, Boston, 2017, pp. 131–132.

[33] I. Romdhani, Chapter 7 - Existing security scheme for iot, in: S. Li, L.D. Xu (Eds.), Securing the Internet of Things, Syngress, Boston, 2017, pp. 119–130.

[34] S. Li, Chapter 5 - Security Requirements in iot architecture, in: S. Li, L.D. Xu (Eds.), Securing the Internet of Things, Syngress, Boston, 2017, pp. 97–108.

[35] S. Li, Chapter 4 - Iot node authentication, in: S. Li, L.D. Xu (Eds.), Securing the Internet of Things, Syngress, Boston, 2017, pp. 69–95.

[36] S. Li, Chapter 3 - Security and vulnerability in the internet of things, in: S. Li, L.D. Xu (Eds.), Securing the Internet of Things, Syngress, Boston, 2017, pp. 49–68.

[37] B. Kitchenham, S. Charters, Guidelines for Performing Systematic Literature Reviews in Software Engineering, Technical Report, Keele University and Durham University Joint Report, 2007. [Online]. Available: http://www.dur.ac.uk/ebse/resources/Systematicreviews-5-8.pdf.

[38] M. Conti, A. Dehghantanha, K. Franke, S. Watson, Internet of things security and forensics: challenges and opportunities, Future Gener. Comput. Syst. 78 (2018) 544–546. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17316667.

[39] T. Mehmood, H.B.M. Rais, Machine learning algorithms in context of intrusion detection, in: 3rd International Conference on Computer and Information Sciences (ICCOINS), IEEE, 2016. [Online]. Available: https://doi.org/10.1109/iccoins.2016.7783243.

[40] M.H. Bhuyan, D.K. Bhattacharyya, J.K. Kalita, Network anomaly detection: methods, systems and tools, IEEE Commun. Surv. Tut. 16 (1) (2014) 303–336. [Online]. Available: doi: 10.1109/surv.2013.052213.00046.

[41] A.A. Diro, N. Chilamkurti, Distributed attack detection scheme using deep learning approach for internet of things, Future Gener. Comput. Syst. 82 (2018) 761–768. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17308488.

[42] A. Ramos, M. Lazar, R.H. Filho, J.J.P.C. Rodrigues, Model-based quantitative network security metrics: a survey, IEEE Commun. Surv. Tut. 19 (4) (2017) 2704–2734. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17308488.

[43] J. Granjal, E. Monteiro, J.S. Silva, Security for the internet of things: a survey of existing protocols and open research issues, IEEE Commun. Surv. Tut. 17 (3) (2015) 1294–1312 [Online]. Available, doi:10.1109/comst.2015.2388550.

[44] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: a survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tut. 17 (4) (2015) 2347–2376 [Online]. Available, doi:10.1109/comst.2015.2444095.

[45] M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas, J. Lloret, Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in IoT, Sensors 17 (9) (2017) 1967 [Online]. Available, doi:10.3390/s17091967.

[46] Y. Fu, Z. Yan, J. Cao, O. Koné, X. Cao, An automata based intrusion detection method for internet of things, Mob. Inf. Syst. (2017) 1–13.

[47] R.K. Gunupudi, M. Nimmala, N. Gugulothu, S.R. Gali, Clapp: a self constructing feature clustering approach for anomaly detection, Future Gener. Comput. Syst. 74 (2017) 417–429. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X16308718.

[48] G.C. Flauzac O., F. Nolot, New security architecture for iot network, Procedia Comput. Sci. 52 (Supplement C) (2015) 1028–1033.

[49] M. Lppez-Benitez, T.D. Drysdale, S. Hadfield, M.I. Maricar, Prototype for multidisciplinary research in the context of the internet of things, J. Netw. Comput. Appl. 78 (2017) 146–161. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804516302922.

[50] H. Sedjelmaci, S.M. Senouci, M. Al-Bahri, A lightweight anomaly detection technique for low-resource iot devices: a game-theoretic methodology, in: IEEE International Conference on Communications (ICC), 2016, pp. 1–6.

[51] P. Levis, N. Lee, M. Welsh, D. Culler, Tossim: Accurate and scalable simulation of entire tinyos applications, 2003.

[52] M.A.A. Cruz, J.J.P.C. Rodrigues, J. Al-Muhtadi, V.V. Korotaev, V.H.C. Albuquerque, A reference model for internet of things middleware, IEEE Internet Things J. 5 (2) (2018) 871–883 [Online]. Available, doi:10.1109/jiot.2018.2796561.

[53] P. Bellagente, P. Ferrari, R.S. Flammini A., E. Sisinni, Enabling profinet devices to work in iot: characterization and requirements, in: IEEE International Instrumentation and Measurement Technology Conference Proceedings 2016, 2016, pp. 1–6.

[54] B. Karakostas, Event prediction in an iot environment using nave bayesian models, Procedia Comput. Sci. 83 (2016) 11–17. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050916301168.

[55] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu, Y. Xiong, X. Cui, Attacks and countermeasures in the internet of vehicles, Ann. Telecommun. 72 (5) (2017) 283–295, doi:10.1007/s12243-016-0551-6. [Online]. Available:

[56] H. Ferreira, G. Cerqueira, J. de Sousa, R. Timoteo, Security analysis of a proposed internet of things middleware, Cluster Comput. 20 (1) (2017) 651–660. [Online]. Available: doi: 10.1007/s10586-017-0729-3.

[57] P.A. Lavrova D., V. Gluhov, Applying correlation analysis methods to control flow violation detection in the internet of things, Autom. Control Comput. Sci. 49 (8) (2015) 735–740.

[58] M.A.N.F. Machaka, P., A. Bagula, Using the Cumulative Sum Algorithm Against Distributed Denial of Service Attacks in Internet of Things, Springer International Publishing, Cham, pp. 62–72.

[59] T.L. Chen, Z., C. Lin, A Method for Detection of Anomaly Node in IOT, Springer International Publishing, Cham, pp. 777–784.

[60] J. Hussain, S. Lalmuanawma, Feature analysis, evaluation and comparisons of classification algorithms based on noisy intrusion dataset, Procedia Comput. Sci. 92 (Supplement C) (2016) 188–198.

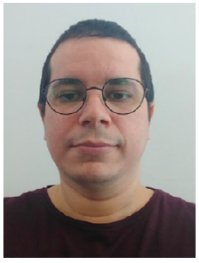
[61] A.S.A. Aziz, S.E. Hanafi, A.E. Hassanien, Comparison of classification techniques applied for network intrusion detection and classification, J. Appl. Logic 24 (2017) 109–118. http://www.sciencedirect.com/science/article/pii/S1570868316300738.

[62] S.L. Gautam, H. Om, Computational neural network regression model for host based intrusion detection system, Perspect. Sci. 8 (2016) 93–95. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2213020916300192.

[63] R.A.R. Ashfaq, X. Wang, J.Z. Huang, H. Abbas, Y. He, Fuzziness based semi-supervised learning approach for intrusion detection system, Inf. Sci. 378 (2017) 484–497. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025516302547.
[64] M.R.G. Raman, N. Somu, K. Kirthivasan, V.S.S. Sriram, A hypergraph and arithmetic residue-based probabilistic neural network for classification in intrusion detection systems, Neural Netw. 92 (2017) 89–97. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0893608017300333.
[65] C.T.K. Fisher W. D., V.V. Krzhizhanovskaya, Anomaly detection in earth dam and levee passive seismic data using support vector machines and automatic feature selection, J. Comput. Sci. 20 (Supplement C) (2017) 143–153.
[66] A.A. Aburomman, M.B.I. Reaz, A novel weighted support vector machines multiclass classifier based on differential evolution for intrusion detection systems, Inf. Sci. 414 (2017) 225–246. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025517307806.
[67] I.S. Thaseen, C.A. Kumar, Intrusion detection model using fusion of chi-square feature selection and multi class svm, J. King Saud Univ. - Comput. Inf. Sci. 29 (4) (2017) 462–472.
[68] J. Arunnehru, M.K. Geetha, Internet of Things Based Intelligent Elderly Care System, Springer International Publishing, Cham, pp. 207–229.
[69] A. Abubakar, B. Pranggono, Machine learning based intrusion detection system for software defined networks, in: Seventh International Conference on Emerging Security Technologies (EST), 2017, pp. 138–143.
[70] M. Almseidin, M. Alzubi, S. Kovacs, M. Alkasassbeh, Evaluation of machine learning algorithms for intrusion detection system, in: 15th International Symposium on Intelligent Systems and Informatics (SISY), 2017, pp. 000277–000282.
[71] E.M. Kakihata, H.M. Sapia, R.T. Oiakawa, D.R. Pereira, J.P. Papa, V.H.C. Albuquerque, F.A. Silva, Intrusion detection system based on flows using machine learning algorithms, IEEE Latin Am. Trans. 15 (10) (2017) 1988–1993. [Online]. Available: doi: 10.1109/tla.2017.8071245.
[72] O. Aslan, R. Samet, Investigation of possibilities to detect malware using existing tools, in: IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), 2017, pp. 1277–1284.
[73] D.A. Effendy, K. Kusrini, S. Sudarmawan, Classification of intrusion detection system (IDS) based on computer network, 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), IEEE, 2017. [Online]. Available: doi: 10.1109/icitisee.2017.8285566.
[74] S.A. Ludwig, Intrusion detection of multiple attack classes using a deep neural net ensemble, in: IEEE Symposium Series on Computational Intelligence (SSCI), 2017, pp. 1–7.
[75] K. Kim, M.E. Aminanto, Deep learning in intrusion detection perspective: overview and further challenges, in: International Workshop on Big Data and Information Security (IWBIS), 2017, pp. 5–10.
[76] Z.Y. Yin X., X. Chen, A binary-classification method based on dictionary learning and admm for network intrusion detection, in: International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2017, pp. 326–333.
[77] P.P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, X. Yi, Privacy preserving internet of things: from privacy techniques to a blueprint architecture and efficient implementation, Future Gener. Comput. Syst. 76 (2017) 540–549. [Online]. Available: doi: 10.1016/j.future.2017.03.001.
[78] A.R. Sfar, E. Natalizio, Y. Challal, Z. Chtourou, A roadmap for security challenges in the internet of things, Digital Commun. Netw. 4 (2) (2018) 118–137. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2352864817300214.
[79] A framework for automating security analysis of the internet of things, J. Netw. Comput. Appl. 83 (2017) 12–27. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804517300541.
[80] F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of things security: a survey, J. Netw. Comput. Appl. 88 (2017) 10–28. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804517301455.
[81] I. Charfi, J. Miteran, J. Dubois, M. Atri, R. Tourki, Definition and performance evaluation of a robust SVM based fall detection solution, in: 2012 Eighth International Conference on Signal Image Technology and Internet Based Systems, IEEE, 2012. [Online]. Available: doi: 10.1109/sitis.2012.155.
[82] X. Guo, N. Ansari, L. Li, H. Li, Indoor localization by fusing a group of fingerprints based on random forests, IEEE Internet of Things Journal (2018) 1. [Online]. Available: doi: 10.1109/jiot.2018.2810601.
[83] Y. Shen, T. Han, Q. Yang, X. Yang, Y. Wang, F. Li, H. Wen, CS-CNN: enabling robust and efficient convolutional neural networks inference for internet-of-things applications, IEEE Access 6 (2018) 13439–13448. [Online]. Available: doi: 10.1109/access.2018.2810264.
[84] A. Azmoodeh, A. Dehghantanha, K.R. Choo, Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning, IEEE Trans. Sustain. Comput. (2018) 1. [Online]. Available: doi: 10.1109/tsusc.2018.2809665.
[85] W.L. Al-Yaseen, Z.A. Othman, M.Z.A. Nazri, Multi-level hybrid support vector machine and extreme learning machine based on modified k-means for intrusion detection system, Expert Syst. Appl. 67 (2017) 296–303. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0957417416305310.
[86] W. Feng, Q. Zhang, G. Hu, J.X. Huang, Mining network data for intrusion detection through combining svms with ant colony networks, Future Gener. Comput. Syst. 37 (2014) 127–140. Special Section: Innovative Methods and Algorithms for Advanced Data-Intensive Computing Special Section: Semantics, Intelligent processing and services for big data Special Section: Advances in Data-Intensive Modelling and Simulation Special Section: Hybrid Intelligence for Growing Internet and its Applications. Available: http://www.sciencedirect.com/science/article/pii/S0167739X13001416.
[87] Y. Zhao, L.T. Yang, J. Sun, A secure high-order CFS algorithm on clouds for industrial internet-of-things, IEEE Trans. Industr. Inf. (2018) 1. [Online]. Available: doi: 10.1109/tii.2018.2816343.
[88] B. Ali, A. Awad, Cyber and physical security vulnerability assessment for IoT-based smart homes, Sensors 18 (3) (2018) 817. [Online]. Available: doi: 10.3390/s18030817.
[89] L. Wang, X. Liu, NOTSA: Novel OBU with three-level security architecture for internet of vehicles, IEEE Internet Things J. (2018) 1. [Online]. Available: doi: 10.1109/jiot.2018.2800281.
[90] H. Wu, W. Wang, A game theory based collaborative security detection method for internet of things systems, IEEE Trans. Inf. Forens.Secur. 13 (6) (2018) 1432–1445.
[91] O.K. Li H., M. Dong, Learning iot in edge: deep learning for the internet of things with edge computing, IEEE Netw. 32 (1) (2018) 96–101.
[92] Q. Yan, W. Huang, X. Luo, Q. Gong, F.R. Yu, A multi-level DDoS mitigation framework for the industrial internet of things, IEEE Commun. Mag. 56 (2) (2018) 30–36. [Online]. Available: doi: 10.1109/mcom.2018.1700621.
[93] S. Majumder, E. Aghayi, M. Noferesti, H. Memarzadeh-Tehran, T. Mondal, Z. Pang, M.J. Deen, Smart homes for elderly healthcarea recent advances and research challenges, Sensors 17 (11) (2017).
[94] A. Rayes, S. Samer, Internet of Things From Hype to Reality: The Road to Digitization, 1st, Springer Publishing Company, Incorporated, 2016.
[95] S.A. Shaikh, H. Chivers, P. Nobles, J.A. Clark, H. Chen, A deployment value model for intrusion detection sensors, in: Advances in Information Security and Assurance, Springer Berlin Heidelberg, Berlin, Heidelberg, 2009, pp. 250–259.
[96] A.A. Gendreau, M. Moorman, Survey of intrusion detection systems towards an end to end secure internet of things, in: IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), IEEE, 2016. [Online]. Available: doi: 10.1109/ficloud.2016.20.
[97] K. Perumal, M. Manohar, A Survey on Internet of Things: Case Studies, Applications, and Future Directions, Springer International Publishing, Cham, pp. 281–297.

Kelton Pontara Augusto da Costa is graduated in Systems Analysis from the Sagrado Coração University (USC). In 2004 received his Master's Degree in Computer Science from the Euripides de Marilia University (UNIVEM). In 2009 he received his Ph.D. in Electrical Engineering from the São Paulo University (USP). During 2010–2011, he worked as a post-doctorate researcher at the Institute of Computing of the University of Campinas (UNICAMP), SP, Brazil. He worked as a post-doctorate researcher at Department of Computer Science of the Paulista Júlio de Mesquita Filho State University (UNESP), SP, Brazil. He is advisor Professor of the Program Master's Degree in Computer Science (UNESP). He is evaluator undergraduate courses (INEP-MEC) and has experience in Computer Science with emphasis in Computer Systems Architecture and Distributed Systems, acting on the following topics: Management in Computer Networks, Security in Computer Networks, Anomaly Detection Systems and Signatures in Computer Networks and Data Flow Analysis in Computer Networks.

João Paulo Papa received his B.Sc. in Information Systems from the São Paulo State University, SP, Brazil. In 2005, he received his M.Sc. in Computer Science from the Federal University of São Carlos, SP, Brazil. In 2008, he received his Ph.D. in Computer Science from the University of Campinas, SP, Brazil. During 2008–2009, he had worked as a post-doctorate researcher at the same institute. He has been a Professor at the Computer Science Department, São Paulo, State University, since 2009, and his research interests include machine learning, pattern recognition and image processing.



Celso de Oliveira Lisboa has a technical-vocational course by the National Service of Industrial Learning - São Paulo. He is graduated in Computer Science from the São Paulo State University, SP, Brazil (2016). Currently is a student in M.Sc. in Computer Science from the São Paulo State University, SP, Brazil.

Roberto Munoz is an associate professor of the School of Informatics Engineering and adjunct researcher at the Center of Cognition and Language (CIDCL) and at the Center for Research and Development in Health Engineering of the Universidad de Valparaíso. Professor Munoz holds doctoral studies in Computer Engineering, as well as Masters in Computer Engineering, Engineering Science, and Education. He is the author of over 50 scientific papers in refereed international conferences and journals. His research areas are focused on Multimodal Learning Analytics, Human-Computer Interaction, and Health Informatics.

Victor Hugo C. de Albuquerque has a Ph.D. in Mechanical Engineering with emphasis on Materials from the Federal University of Paraiba (UFPB, 2010), an MSc in Teleinformatics Engineering from the Federal University of Ceara (UFC, 2007), and he graduated in Mechatronics Technology at the Federal Center of Technological Education of Ceara (CEFETCE, 2006). He is curtrently Assistant VI Professor of the Graduate Program in Applied Informatics, and coordinator of the Laboratory of Bioinformatics at the University of Fortaleza (UNIFOR). He has experience in Computer Systems, mainly in the research fields of: Applied Computing, Intelligent Systems, Visualization and Interaction, with specific interest in Pattern Recognition, Artificial Intelligence, Image Processing and Analysis, as well as Automation with respect to biological signal/image processing, image segmentation, biomedical circuits and human/brain-machine interaction, including Augmented and Virtual Reality Simulation Modeling for animals and humans. Additionally, he has research at the microstructural characterization field through the combination of non-destructive techniques with signal and image processing and analysis and pattern recognition. Prof. Victor is the leader of the Computational Methods in Bioinformatics Research Group. He is an editorial board member of the IEEE Access, Computational Intelligence and Neuroscience, Journal of Nanomedicine and Nanotechnology Research, and Journal of Mechatronics Engineering, and he has been Lead Guest Editor of several high-reputed journals, and TPC member of many international conferences. He has authored or coauthored over 200 papers in refereed international journals, conferences, four book chapters, and four patents.