Industrial Internet of Things Security enhanced with Deep Learning Approaches for Smart Cities

Naercio Magaia, Ramon Fonseca, Khan Muhammad, *Member, IEEE*, Afonso H. Fontes N. Segundo, Aloisio V. Lira Neto, and Victor Hugo C. de Albuquerque, *Senior Member, IEEE*

Abstract—**The significant evolution of the Internet of Things (IoT) enabled the development of numerous devices able to improve many aspects in various fields in the industry for smart cities where machines have replaced humans. With the reduction in manual work and the adoption of automation, cities are getting more efficient and smarter. However, this evolution also made data even more sensitive, especially in the industrial segment. The latter has caught the attention of many hackers targeting Industrial IoT (IIoT) devices or networks, hence the number of malicious software, i.e., malware, has increased as well. In this article, we present the IIoT concept and applications for smart cities, besides also presenting the security challenges faced by this emerging area. We survey currently available deep learning techniques for IIoT in smart cities, mainly Deep Reinforcement Learning, Recurrent Neural Networks, and Convolutional Neural Networks, and highlight the advantages and disadvantages of security-related methods. We also present insights, open issues, and future trends applying deep learning techniques to enhance IIoT security.**

Index Terms—**Deep Learning, IoT, Industrial IoT, Security, Smart Cities.**

I. Introduction

THE underlying concept underneath the Internet of Things (IoT) paradigm is to enhance the modern quality of life. IoT consists of interconnection, through the Internet, of everyday objects equipped with numerous sensors with computing and communication capabilities, which enable them to send and receive information [1].

Temporal and spatial data are collected from IoT sensors and devices, usually from specific events and circumstances tackling various challenges [2]. Nowadays, such devices are evermore smarter, their communication is faster and they are capable of executing more complex tasks [3]. Hence, IoT is used in nearly every field, such as finances, tourism, entertainment, industry, energy distribution, transportation, healthcare, smart cities, education, and even in the domestic environment [4], [5]. Consequently, there are more developers, academia researchers, and individuals working on integrating IoT technologies into commercial operations for smart cities, paying less attention to safety and/or security measures for such devices and networks. Such dereliction can compromise IoT users and, in turn, disrupt an active ecosystem [6].

The undeniable advantages offered to the industrial sector by the IoT paradigm, also known as the Industrial Internet of Things (IIoT), are nonetheless associated with severe security defects. The overlook of several security problems enables the exploitation of sensitive data ranging from unprotected cameras' video streams to the access of confidential data in IIoT devices [7]. Frequently, devices are effortlessly exploited due to the neglect of security aspects and to the design of potentially unprotected systems because of the lack of related legislation along with profit-driven businesses [8].

Ensuring cybersecurity is one of the most significant challenges faced in an IIoT environment in smart cities. Specifically, blocking unauthorized access, enforcing privacy communication, and protecting edge devices from malware attacks are some of the current challenges [9]. Many works in literature propose automated methods based on machine learning (ML) models, including deep neural networks, to guarantee IIoT security regarding malware detection, fault diagnosis, and anomaly detection [10], [11].

The sophistication and magnitude of cyberattacks, especially in the zero-day ones, has been raising and threatening more IoT devices, as the application of such systems affects peoples' lives and becomes more critical as more sensitive data are shared. Plentiful and significant targets including industrial control, smart cities transportation, healthcare, smart grid, and other wide-scale systems make very appealing for bad-intended foes [12]. These attacks, born from the physical connection of smart devices or inherited from the already known digital environment, threaten the daily lives and the proper function of the sort of device, including denial of service attacks or bumping data to gaining access to the local system [13].

The propagation of neural networks has called out for better security solutions, making ML a promising technology to solve the above issues. The neural networks' proliferation posed

Manuscript received June 28, 2020; revised November 21, 2020; accepted November 30, 2020. This work was supported in part by the Institute of Information communications Technology Planning Evaluation (IITP) grant funded by the Korea government (MSIT) (2019-0-00136, Development of AI-Convergence Technologies for Smart City Industry Productivity Innovation); and in part by the Brazilian National Council for Research and Development (CNPq) under Grant 304315/2017-6 and Grant 430274/2018-1. It was also sponsored by FCT through the LASIGE Research Unit, ref. UIDB/00408/2020 and ref. UIDP/00408/2020. (Corresponding author: Khan Muhammad, Naercio Magaia)

N. Magaia is with LASIGE, Department of Computer Science, Faculty of Sciences, University of Lisbon, Campo Grande, 1749-016 Lisbon, Portugal. (e-mail: ndmagaia@ciencias.ulisboa.pt)

R. Fonseca and A. Neto are with the University of Fortaleza, Fortaleza – CE, Brazil. (emails: ramon.rbf@edu.unifor.br and aloisio. neto@supesp.ce.gov.br)

V.H.C. Albuquerque is with LAPISCO, Federal Institute of Education, Science and Technology of Ceará, Fortaleza 60811-905, Brazil, and also with the ARMTEC Tecnologia em Robótica, Fortaleza 60811-341, Brazil. (email: victor .albuquerque@ieee.org)

A. Segundo is with Department of Computer Science and Engineering, Chalmers and the University of Gothenburg, Gothenburg, Sweden. (email: afonsohfontes@gmail.com)

Khan Muhammad is with the Department of Software, Sejong University, Seoul 143-747 South Korea (e-mail:khan.muhammad@ieee.org)

the need for providing some intelligence to the machines to gather information out of the data collected by sensors. The purpose is to make the appropriate decision more intelligently and autonomously [13], [14] and therefore forced by the envisioned applications directing at achieving smart houses, smart factories, smart hospitals, and smart grid, among others. The response to such a demand is embodied by Deep Learning (DL), which depicts an evolution of the conventional neural network solutions [15].

DL is an emerging method applied in numerous IIoT applications. It offers smart decision-making and rationalization and is based on Artificial Neural Networks (ANN) [16], [17]. It is trained using large volumes of labeled data and seamlessly updating related model parameters [7]. One of the main techniques and often used is the Convolution Neural Network (CNN), consisting of a series of fully connected layers in which it applies a series of convolution layers with filters (i.e., Kernals) with Pooling and Softmax function to enhance the recognition and predictions [18].

The specific contributions of this article are summarized as follows:

- We present the IIoT concept, its generic as well as DL-enabled applications for Smart Cities, besides also presenting the security challenges of this emerging area.
- We survey currently available DL methods for IIoT in smart cities and highlight security-related methods as well as describing their advantages and disadvantages.
- We also present insights, open issues, and challenges for applying DL techniques to enhance IIoT security.

The remainder of this article is as follows. Section II briefly introduces the concept of IIoT, its applications, and the challenges of securing such a system. Section III describes and comments on the various DL methods applied in the security of IIoT. Section IV highlights what has been accomplished so far, besides presenting challenges and open issues. Section V presents concluding remarks and our vision of future research directions.

II. IIoT concept, applications, and security challenges

A. The IIoT concept

IIoT relates to interconnected machines, networked devices, and control sensors, commonly with applications of industrial computers, including production and power management. This interconnection between devices provides for improved analysis, compilation, and exchange of data, conceivably facilitating improvements in performance and productivity [7].

Consolidation in a conventional IIoT system with future-oriented technologies includes fog computing, artificial intelligence (IA), big data analytics, and more, aiming to improve services, management, and governance in smart cities [19], [20]. Utilizing embedded systems, wearables devices, and wireless sensor interfaces allow IIoT to continuously and ubiquitously acquire raw data.

Li et al. [21] proposed a general architecture for IoT composed of five layers, namely: perception, network, middleware, application, and business. IIoT devices are in the perception layer and usually operate in exposed areas. The network layer is the connection layer in the sense of transmission of data and typically is composed of servers and access points. The middleware is where the brain and fully-fledged ML applications operate. The application and business layers are the closest to the users and are generally composed of software and general applications. Figure 1 shows a general representation of a five-layer IIoT architecture.

In the smart city context, all types of sensor are used in the Perception layer, from a simple smoke detector sensor [22] to a complex multi-view camera setting [23], as well as any device that can capture some form of data, such as wearables with a cardiac sensor [24]. The main objective of this layer is to capture data so the higher layers can use it. Technologies such as smart streetlights and video monitoring and processing are some examples that depend heavily on sensors of the perception layer.

The Network layer focuses on data transfer and transportation and the devices to enable it. Access points communicating through a wired and wireless connection or antennas, providing a mobile connection as 5G [25] and servers to collect and process the information. Some technologies, such as Network Function Virtualization and Virtual Network Functions, work directly in this layer.

The Middleware layer is a concept of systems and software that runs mostly in servers that provide some service to the higher layers but also uses the data collected by the perception layer. This software and services tend to be computationally demanding, such as training a new ML model. Besides, most of the security techniques are applied in this layer as it provides the intersection between the software and the local hardware [26].

The Application and the Business layers provide the software and the clients for the end-user. The context of both layers can be different, but the challenges faced are mostly the same. Resource allocation, secure data transmission, and mobility management are the primary concerns [27].

B. Applications

1) Generic applications for Smart Cities: One of many applications that smart city aims, is the smart streetlight. A system that can manage and control the streetlights is capable of reducing the energy consumption by lighting the street only when there is a traffic/pedestrian, or dimming the lights depending on the time and weather. For the realization of such a smart system, it is necessary to equip streetlights with sensors and connectivity or processing power to collect and treat data so that it functions effectively. The data can be processed locally or transmitted to a control system through the network, in which case, the system will determine the best approach. This system is already in use in some cities such as Amsterdam in the Netherlands and San Jose in the United States [28]. Discussing in detail the Amsterdam case, lamp posts were equipped with various sensors such as cameras, WiFi connections, environmental sensors, among others. Applications were then developed using DL and computer vision (CV) techniques to be deployed, allowing to provide

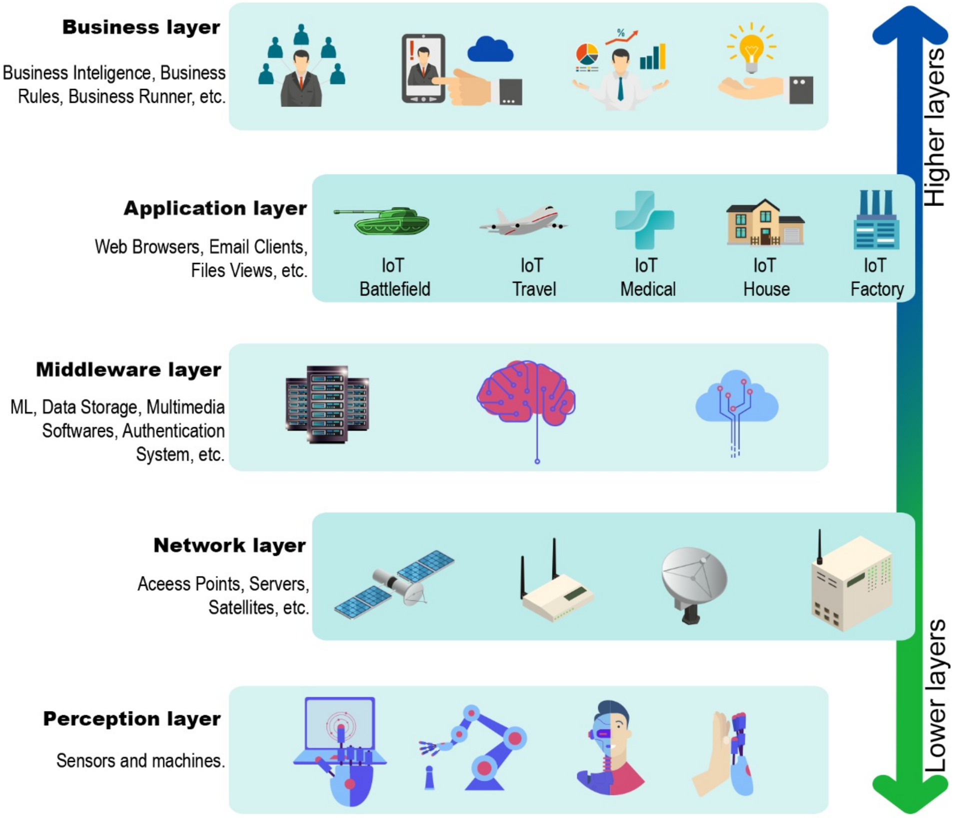

Business layer
Business Inteligence, Business Rules, Business Runner, etc.
Application layer
Web Browsers, Email Clients, Files Views, etc.
IoT Battlefield
IoT Travel
IoT Medical
IoT House
IoT Factory
Middleware layer
ML, Data Storage, Multimedia Softwares, Authentication System, etc.
Network layer
Aceess Points, Servers, Satellites, etc.
Perception layer
Sensors and machines.
Higher layers
Lower layers

Fig. 1. General representation of a five-layer IIoT architecture.

information such as crowds, traffic, parking conditions, and air quality, besides being able to adjust the brightness and color of the lamp remotely and dynamically according to different conditions.

A common problem in big urban areas is high vehicle density. To provide an efficient and safer route is a constant struggle in a smart city environment. Therefore, deploying a Smart Traffic Management is one of the main goals as it enables alleviating the issue mentioned above [29], [30]. Various technologies can be used to enhance such system, extending from a simple and less complex one, e.g., car navigation and signals traffic control, to a highly complex one, e.g., multiple closed-circuit Television Camera (CCTV), all integrated with live data, DL techniques and computer vision (CV), to produce a real-time decision-making system providing guidance and statistics for further analysis. A case in Boston is a reference for smart traffic [25]. In this case, the primary goals were to reduce carbon emissions, analyzing and reducing vehicle distance travel, and make data accessible to residents. It was divided into four categories, specifically: unlocking data, sharing data, analyzing data, future vision. The first category, Unlocking data, is to install cameras and sensors in the street that are capable of capturing information and transfer it to a Control and Management Center. The second is responsible for transmitting the data collected in the center to a department so it can be analyzed, leading to the third category, analyzing data, in which, applying DL techniques, provides consolidated information. The last category, future vision, is a roadmap to develop and deploy new technologies to improve the overall system.

Smart grids, in particular smart meters, is an area that drives much attention for its enormous potential and benefits [31]. Providing a reliable service while having to continually adjust to new regulations, for instance, reducing carbon emissions and still be flexible to customer demands, is a challenge that many companies seek to implement. Novel concepts like Virtual Power Plants (VPPs) have been developed to address pricing, load reduction, and demand response issues. The latter concept consists of using a group of customers and putting them under a cooperative program in order to predict better, analyze the demands, and use the collected data to further enhance the system [32]. The key is in the management system, which centralizes all the information, collecting the data from sensors installed in some transmission lines. The data then can be analyzed and both DL and business intelligence can be applied to provide a better understanding and control of storage and generation as well as the distribution and predictions.

The current healthcare system faces substantial challenges, and it struggles to provide a good quality service at a low cost for the increasing demand and the high cost of keeping such an environment [28]. Besides, the IoT paradigm offers solutions to these challenges through devices capable of monitoring the patient's activities and signals. These devices can be sensors attached to the patient's body or in the surrounding environment, measuring signals such as blood pressure and heart rate to the vigilance of activities and predicting behaviors with DL [33]. An example is online cardiac monitoring [4] that collects and analyzes heart signals and can predict future problems. When integrated with a smart healthcare system, they can fire a signal alert to an ambulance and can inform the hospital of a possible emergency.

2) DL-enabled applications: Numerous IoT and IIoT applications are employing the DL concept ranging from data mining of surveillance videos [34] to user authentication in the physical network layer [35], [36]. The excellent features of DL are the enormous capacity of recognizing patterns, which leads to many applications in smart cities. One of the problems that DL and other types of Artificial Intelligence (AI) have is that they need to have a vast amount of labeled data before they start to learn. Besides, depending on the type of data, they can also require a vast amount of computing power to process it.

With this in mind, Gao et al. [37] have developed a method to detect the saliency map, which is an image that shows each pixel's unique quality, of collaborative cameras (also called co-saliency) to increase the trust of each sample frame of the stream video, making the data secure and resumed for another AI technique to learn from it. This application can go to all areas of IoT, from smart-homes that use surveillance cameras to smart cities in detecting traffic and industrial surveillance of employees. Although the method mentioned above has been used for surveillance, there are numerous applications where it can be applied in IoT and IIoT [38].

If we consider the variety of applications making use of DL and IoT concepts, it is essential to notice the security flaws and breaches of an application to handover some confidential information or cause material damage, or even endangering lives, especially in industrial smart city applications [39], [40]. For example, invading some security cameras can cause sensitive data leakage. Moreover, deployed IoT sensors at factories control environmental contamination and substance exposures in water supply, while sensors of noxious gases, smoke, and temperature, in addition to alarm systems, prevent environmental disasters [41]. Some case studies have described the notable influence of IoT on natural resources' integrity and consumption.

There are numerous security implications in this context since IIoT is widely heterogeneous by nature. While the research contributions of [29], [42] mainly discuss the topics of IoT structures and similar technologies, several other studies delved deep into its security features.

C. Security Challenges

Several technological challenges, including restricted storage, power, and computational capabilities, pose many IoT security conditions. For instance, the simple effect of unauthorized access to IIoT devices by using default user credentials remains unsolved [43]. Although the manufacturers are aware of this flaw, little is being done to mitigate it, thus burdening the user with a technically challenging problem. Ironically, in IoT devices, and as shown by Li et al. [32], about 48% of users are unaware that their devices could be used somehow to conduct cyber-attacks, and firmware updates are never performed in 40% of them. Many have argued that the updates should be the responsibility of the manufacturers and software developers in order to remediate security risks.

As previously mentioned, the IIoT architecture can be divided into five layers, each layer having its own vulnerabilities. In the perception layer, IIoT devices are vulnerable to various physical attacks since they operate in the exterior environment, and the primary goal of an attacker usually is to steal or tamper sensors' data. Attacks such as man-in-the-middle attacks and denial of service (DoS) happens in the middleware and network layers. Business and application suffer the same types of attacks of a traditional computer, and some examples include privilege escalation and structured query language (SQL) injections. Figure 2 shows possible attacks at each layer.

The main issue in IoT is the lack of communication standards [44], which complicates the task of ensuring security given the inexistence of guidelines. Consequently, the development of general solutions can be troublesome regarding security features. As shown by S. Garg et al. [45], the focus of hackers is to attack the application layer (i.e., software) and web servers. The reasons behind it are that servers accumulate a significant amount of private information, besides being the gateway to other devices. Therefore, injecting malicious code that is able to infect the connected equipment is potentially valuable to hackers.

In terms of hardware, two features directly involve hardware security techniques: a hardware root of trust and hardware-supported software isolation [46]. The idea of using the hardware as a mechanism to generate units isolated from one another and to save cryptographic keys securely are not new and are comparable to those in classical IT studies. Many challenges emerge in hardware security in smart cities' IIoT systems, mainly because of their computational and energy restrictions. Moreover, by nature, some IIoT devices might not possess accurate real-time clocks, making some networks fundamentally impossible. These factors can cause even higher-layer security to be compromised [47].

On the other hand, and regarding software, there are other challenges. For instance, current operating systems (OS) support process isolation, that is, one process cannot interfere with another one on the system. The memory management unit (MMU) can guarantee such isolation. The issue here is to maintain the classic process isolation idea without an MMU since there is no centralized OS managing all processes in an IIoT environment [48]. To allow IIoT devices with more resources, there are necessary new methods to enable the OS of resource-constrained to be able of such isolation, even though the notion of process isolation is well-known.

Another typical challenge is access control. The OS from untrusted code through access control protects system resources. There are generally two concepts to secure the access. The first is to designate part of the code a unique identifier that only the OS knows. The second is to give a token where only the process with it can run. Access control systems are particularly challenging to make [43]. The access control concept, although still pertaining to IoT platforms, poses new

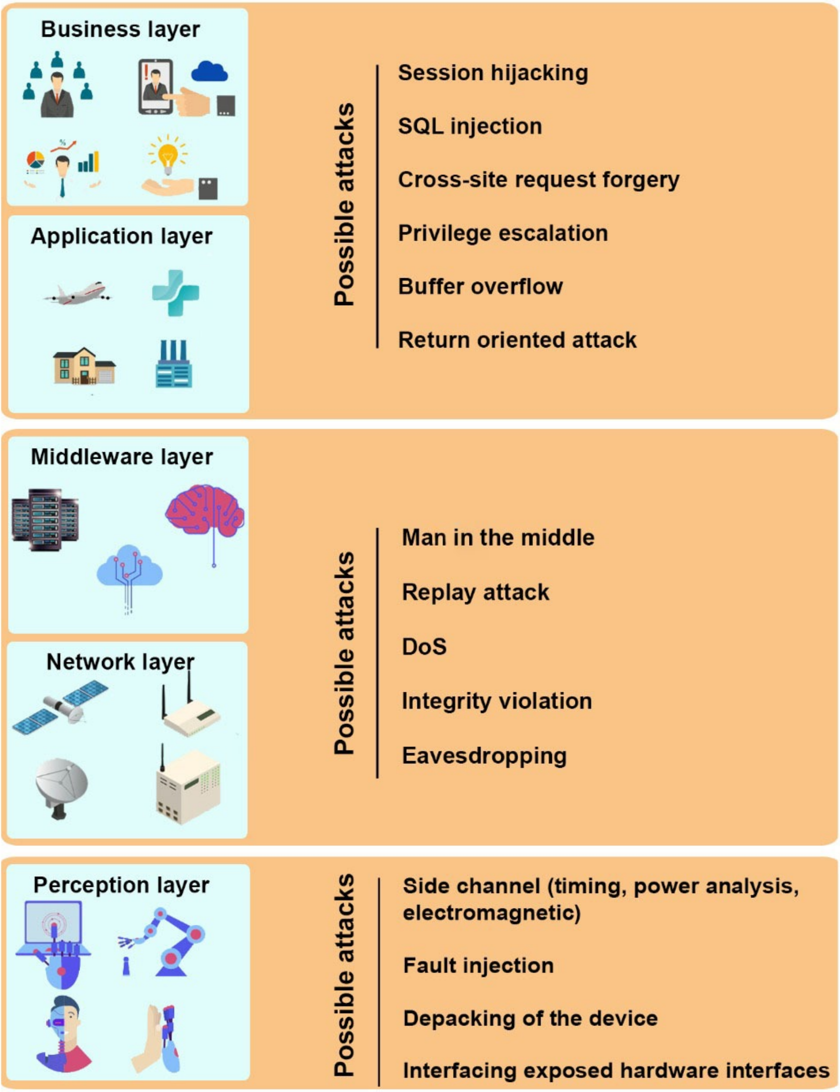


Fig. 2. Representation of the possible attacks per layer in an IIoT architecture

challenges from a usability perspective in the design of these systems. An intriguing challenge is to produce an access control system for IoT while utilizing our natural intuition about physical objects as most of the previous access control systems still utilize files and processes, and virtual objects [49].

Authentication also plays a critical role in IoT security. Passwords are currently the most popularly used forms to authenticate users to their IoT devices, services, and platforms. However, weak passwords cause a lot of concerns as they recently enabled massive botnets DoS attacks [50], [51].

Multiple computing areas use techniques for detecting misbehaving devices on the network as a comprehensive and well-deployed security manner. Obtaining useful information from anomaly detectors is the core challenge for tuning them to generate a low amount of errors, which means to reduce how frequently the algorithm returns a false-positive or false-negative [52]. The heterogeneity of the devices that typically connect to a network makes this particular case a challenging problem. Since most of them perform different functions, which leads to complex network traces, making it hard to characterize "bad" behaviors. On the contrary, IIoT devices have simple goals, aiming to a more straightforward network dynamics, therefore, leading to easy to predict behavior models and eventually leading to fewer errors in anomaly detectors [53].

III. Deep Learning for IIoT

Deep Machine Learning (DML), or just DL, plays an essential role in IIoT, as the characteristic versatility of the technology allows the deployment in almost all fields, of which we will describe some of the key topics here. Figure 3 shows the working principle of DL applied to IIoT security.

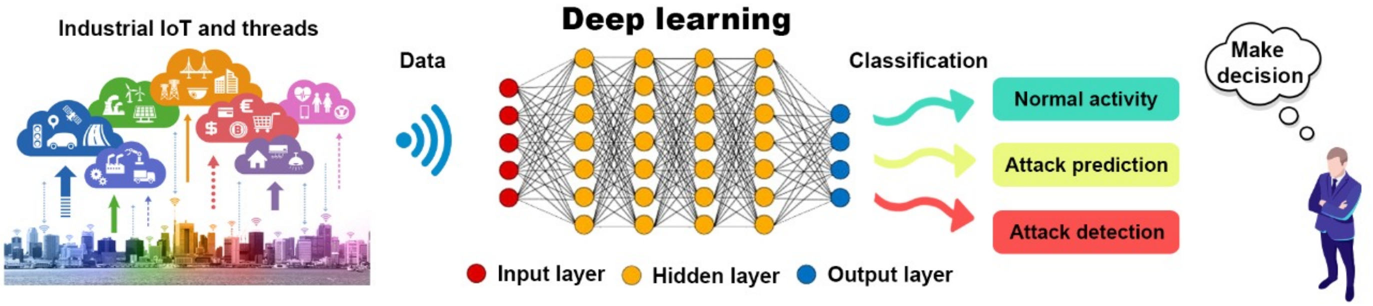


Fig. 3. An illustration of DL working principle for IIoT Security

A. Resource Management

Network Function Virtualization (NFV) [54] has been mostly employed by network service providers to separate dedicated hardware from network functions by running on general hardware functions inflexible software applications as Virtual Network Functions (VNFs). However, such technology has some limitations. The orchestration of Service Function Chain (SFC) [54] is the major challenge in NFV as it is the pipeline operation of VNFs. The efficiency of physical resource usage and service provision is critically affected by the placement and organization of SFC. SFC faces challenges in dynamic service mapping and service reliability and dynamic traffic regulation [55].

SFC orchestration optimization is supported by techniques such as heuristic algorithm, integer linear programming (ILP), and game theory. However, the orchestration problem is that it grows exponentially and is even more noticeable in complex networks. The latter is also resource-demanding as the network increase, leaving the previous methods to be lacking in the necessary scalability. In order to reduce the load in the servers, a common and prominent technique is the Mobile Edge Computing (MEC). However, the end-to-end connection latency caused by the physical distance between terminal devices and cloud service providers is known to be intolerable or impractical in sensitive applications of latency [54].

To address the SFC orchestration problem, Shaoyong et al. [54] used Deep Reinforcement Learning (DRL) as a solution, besides also implementing the Asynchronous Advantage Actor Critic (A3C) algorithm in the hybrid cloud-edge scenario to optimize SFC orchestration. They also combined SFC allocation, after obtaining the optimal orchestration, with Blockchain to ensure reliability on the process of SFC allocation. This allowed for a very efficient, scalable, and secure resource management. Nonetheless, any heterogeneity and delay of response are omitted.

On the other hand, Fatima et al. [56] proposed an approach in the IIoT network, where the devices' session setup and management, channel allocation, and interference management are in the underlay networks. The survey shows great potential using DRL to solve the resource management issue, detailing the challenges and possible solutions, although it lacked applications.

Lu et al. [57] described a series of system designs for improving communication and resources management considering a 5G network architecture. The limitation that usually undergoes in edge and mobile devices, such as limited storage space or insufficient power supply, is a decisive factor to not accommodate network equipment growth. The use of expensive and inflexible equipment by network operators, besides a series of complex control plane protocols, are the main factors influencing the slow upgrade of network equipment.

To effectively reduce latency, network overhead, and packet size, Lu et al. [57] proposed an ML-based recommender system to predict the most suitable packet, meeting the user's demand based on the historical consumption record. According to their testbed's results, the algorithm improved the mobile data usage in reducing the data transferred, latency, and overhead in certain regions. However, incomplete data and irregular user behavior directly impact the algorithm, making it, in some cases, not only fail to predict packets but also to increase the resources needed for routing since it needs to send more metadata to the recommender's prediction, hence demanding improvement in efficiency and availability.

Although the previous algorithm targets generic 5G-enabled applications, it is not well suited for some specific ones, such as vehicular communication. With this issue in mind, Khan et al. [58] developed an ML-enabled architecture for secure and robust communication between autonomous vehicles. The need to collect real-time information about speed, direction, and location, with the increasing demand for data services and high bandwidth because of frequent updates, are the main requirements for vehicular communication creating several challenges to overcome. The proposed policy framework architecture for resource allocation in SDN-based 5G cellular networks uses three approaches: CNN, LSTM, and DNN. The experimental results show that it was possible to improve resource allocation time and accuracy. Specifically, LSTM and CNN approaches were better in resource allocation time and accuracy, respectively.

B. Authentication Systems

A significant number of IoT devices operate under untrusted environmental conditions, therefore, exposed to several potentially malicious attacks [8]. Traditional methods have high computational cost and lack protection from dynamic injection attacks in which the intruder can collect data in both, long time duration and stealthy to the system.

B. Chatterjee et al. [8] proposed a watermarking framework that enables the IoT gateway to authenticate IoT devices signals and detects the existence of a cyber-attack using augmentation. It exploits variations on the manufacturing process in order to create a unique and device-specific identifier for a physical system, called Physical Unclonable Functions (PUF). This work's results are robust and reliable, although there is no comparison to other methods and heterogeneity.

Another example demonstrated in [36] uses authentication in the physical layer by comparing channel impulse response, such as channel state information, channel phase response, and received signal strength as the comparison is performed using a threshold, hence making it harder to authenticate where there are multiple nodes at the same time. The solution is to use Deep Neural Network (DNN) for faster and scalable authentication, which allowed for impressive results. However, it lacks proper studies in using the method in more secure environments.

Other studies such as [59] and [11] also show impressive results in the field of authentication, as both use DL to improve the classification and identification in an ample amount of simultaneous or complex data. However, some improvements in dealing with static devices and finding a good tradeoff between resource constraints, delay, and robustness are still necessary.

C. Surveillance

Vision sensors installed in a smart city network can generate enough video data to meet Big Data requirements, being also critical devices for various IIoT applications. This data requires high processing power for tasks such as street monitoring and salient events detection in the public areas. Redundancy removal, along with presentation and preservation of only salient data in compact form, is the essential requirement of such applications. Otherwise, it would be impractical to perform such tasks in smart cities for future use and analysis. Santana et al. [60] proposed CNN approaches based on the UNet architecture and Siamese ANN for scene change detection and obstructed routes applications. These approaches consist of an encoder and decoder, where the former is responsible for finding the difference between images while the latter interprets them to generate a binary mask. The experiments show robust and promising results, even considering complex scenarios, such as bad weather conditions. The downside is that the network requires a clear and distinct difference in the images for detection. If the changes are too subtle or minimal, the accuracy might be unacceptable.

In this same context, Gao et al. [61] proposed a salient object detection CNN in the cloud-edge environment. The key is to maintain the detailed local information on the edge but extracting the global contextual information on the cloud. To this aim, the training stage was structured in hierarchical allocation, so it would be possible to extract the within-semantic and cross-semantic knowledge. The proposed algorithm was divided into two pyramidal structures, i.e., the forward and backward pyramids, to detect the saliency. The former pyramid aims to extract the global contextual information and preserve the detailed local information in the raw image. The latter one aims to fuse the different-level features from the forward pyramid to predict the saliency map of the raw image. This approach was compared to eleven other state-of-the-art methods, showing the performance and accuracy of the algorithm, although it is not suitable for resource-constrained devices.

Another algorithm was proposed by Santana et al. [38] for saliency detection, which consists of two mechanisms. One is the region-proposal-based optical flow in order to address the blurriness of moving background disturbance. The other mechanism is the bidirectional Bayesian state transition for overcoming the difficulty of modeling the saliency uncertainty in the spatio-temporal domain. The experiments were performed with two public datasets, and the results performed slightly better than other state-of-the-art algorithms.

Studies on summarization, such as in [62], which uses a DL-based method to achieve Multi-View Summarization (MVS) by means of a target-appearance-based shots segmentation and extraction of deep features from each frame of a sequence, eliminate major data storage overload and cutting the essential parts of a video. For an online MVS to work correctly, it is required to have a large network bandwidth and a considerable computational power for an IIoT device. Although the onerous requirements for the method, the results show that it has been able to cut an enormous amount of useless data. Hussain et al. [3] use a similar MVS approach but applied to embedded devices.

Muhammad et al. [63] tried to solve costs in power and energy by applying Hierarchical Weighted Fusion, which is a mechanism designed to produce an effective extraction of representative keyframes by aggregating scores for each frame of the segmented shot and smartly combining the extracted features. Moreover, in [64], they tried to solve the cost in scenarios of resource-constrained devices. Gao et al. [37] presented a method to detect and extract the co-saliency of video streams in IIoT.

Events such as fire disasters are also important to monitor in a surveillance environment, as, for instance, they can lead to social and economic loss. Due to this reason, fire detection systems are essential to develop, and significant research efforts have been made to prevent, detect, monitor, and generate necessary alarms about the existence of smoke and fire. However, this detection has numerous challenges that restrain the performance of AI-assisted applications.

Most smoke detection methods can be classified into three categories, namely color-based, motion-based, and a hybrid approach [65]. The color-based methods use the color model, a mathematical expression to describe the color separating into three or four different values, to detect specific patterns to identify fire or smoke such as a specific black cloud or a bright spot. The motion-based methods use the smoke locomotion to predict fire and differentiates from the fog and other natural events. The hybrid methods combine both to increase the probability of detection.

As an example, Muhammad et al. [65] proposed an energy-friendly MEC-assisted smoke detection based on a deep CNN. The method consisted of a light-weighted architecture, and one of the main features is to be deployable in foggy surveillance environments. This method presents acceptable accuracy and execution time. However, this approach only detects smoke, but not its location. Similarly, Khan et al. [66] developed a smoke detection method with local processing for assistance and real-time detection in a foggy environment. Even though suffering the same restrictions as other approaches, their results were better in terms of false alarms, besides being able to detect even in the early stages of fire.

D. Privacy Awareness

Data privacy plays a critical role in smart cities, and the following two main security concerns must be taken into account when talking about privacy [67]. The first one is data privacy leakage, which can prevent participants from sharing their data since it can be disclosed. The second is the model parameters' privacy leakage. This case will compromise the training model, which can cause harm in the interests of the collective participants since the training model is considered the intellectual property of the participants and should not be revealed to others, making it untrustful [68].

Ensuring privacy comes at the cost of performance since the system must check for all possible leakages, making data transition slower. To prevent this, He et al. [69] developed a new method that was called Deep post-decision state (PDS) learning capable of exploiting the extra information about the energy harvesting process that outperforms most conventional methods with few downsides, such as the slower speed learning.

Zhang et al. [7] described the problem when facing a lack of a massive public dataset in a learning group to share this data in an asynchronous environment, which can cause the private information to be exposed. Thinking about this problem, the authors presented two approaches to address this issue, one for continuous and another for dynamic systems. Both methods are based on five main components, which are "KeyGen" (to produce the private/public key pair), "Decryption", "Compute", "Encryption", and "Aggregate" (the learned data to the model). Both approaches presented good results, however, coming with some computational cost. Liu et al. [70] arrived at similar results. Privacy-preserving mechanisms were proposed in [71], [72] to enable mobile IoT devices (e.g., vehicles) to make routing decisions while keeping their sensitive data private.

Another critical factor is Blockchain, with the capability of offering unique properties such as transparency and data integrity [73]. In smart cities, vehicular networks and intelligent transportation systems' applications have critical data and thus need to preserve privacy. A federated learning (FL) technique integrated with Blockchain was presented by Lu et al. [74] endeavoring for privacy-preserved data sharing in IIoT. The authors implemented ML into the consensus process of the Blockchain, where, by removing the centralized trust, it was capable of improving the resources management of the device as well as the efficiency of the transaction. Despite the promising results, data privacy could not be guaranteed. Besides, Blockchain's computational requirements is still a demanding challenge and a limiting factor.

Similarly, Zhao et al. [75] also used FL but aiming to enable MEC's server and mobile phones to use privacy-preserving communication. To reduce the substantial computational resource demanded by both ML and Blockchain, the authors proposed a new normalization technique.

E. Attacks and Threads Detection

Considering the five-layers' architecture proposed by Li et al. [21], IIoT devices in the perception layer are vulnerable to several physical attacks, mostly aiming to steal or tamper the data that these sensors collect [28]. However, it is mostly used with another device in the local area. The vulnerabilities in the network layer often result in attacks such as man-in-the-middle and DoS [26]. Such attacks mostly result in exploiting security vulnerabilities of protocols such as TCP/UDP and Domain Name System (DNS) [76]. Traditional computer systems and the application layer share much in common; therefore, they both are plagued by the same types of attacks and vulnerabilities, for instance, SQL injections, depending on the application [77].

1) Malware Detection: In short, malware is a malicious software or a code that is injected in a device to various ends, such as sending data to others or facilitating the access of more harmful threads (the famous Trojan). To prevent this, Ullah et al. [78] described a DL method capable of preserving privacy awareness and detecting malware threats. This method was compared to four other methods, namely the k-nearest neighbors' algorithm (KNN), Latent Semantic Analysis (LSA), Parse Tree, and Multiple Linear Regression (MLR). Although LSA performed better, it was not able to scale when compared to the presented DL based method.

Azmoodeh et al. [79] used Deep Eigenspace Learning (DEL) to detect malware on devices by analyzing the operational code sequence. This method outperformed other ones presented in the paper in both precision and accuracy. However, the method came to a higher computational cost and a shortcoming in terms of distributed computing. On the other hand, Alasmary et al. [52] proposed a method using Control Flow Graphs (CFG) to detect malware. However, although being lighter, its performance was surpassed by another method that used DL by 96% to 99% accuracy, respectively, and it was tied to a specific OS (i.e., Android).

2) Attack and Intrusion Detection: An attack and intrusion have a similar goal, which is to enter the system of the device and steal or write data onto it in order to gain or destroy the information or the system [80]. A. Diro et al. [41] applied a DL technique in a fog computing environment, distributing the detection on fog nodes, getting better physical resource management and scalability. Although promising with results around 99% of accuracy and precision, it requires a large amount of network bandwidth. M. Aminanto et al. [81] proposed a deep-feature extraction and selection approach that combines stacked feature extraction and weighted feature selection. The proposed approach achieved a very high detection accuracy and a very low false alarm rate in comparison to other feature selection methods such as Completely Fair Scheduler (CFS), ANN, Support Vector Machine (SVM), and C4.5 algorithm in Wi-Fi networks.

Li et al. [32] described two DL methods that work together to extract energy auditing data effectively, enabling for a physical and cyber detection of attacks. The paper does not mention any test, only proves the concept using predefined cases.

3) Anomaly Detection: Anomaly Detection is a broader spectrum since it can take many forms, although with a similar symptom. That is, in the network traffic data, it is possible to identify suspicious activity such as malicious queries or a DoS attack through pattern recognition. In many studies such as [13], [45], although having different goals, they used network traffic data or energy oscillation and came to similar results. All the proposed methods had accuracy ranging from 96% to 99.9% in determining a system anomaly, nonetheless omitting key factors such as the system response time and bandwidth usage, leaving these factors as an open issue.

N. Magaia et al. [82], [83] proposed an AI-based reputation framework, which used ML and the artificial immune system, for misbehavior detection in vehicular environments. Besides outperforming state-of-the-art reputation systems in the experimental setup considered, the proposed framework presented very low false positives and negatives' ratios.

Table I summarizes DL techniques for IIoT. The contribution made by the research community in enhancing the security have taken good steps in order to preserve the integrity of a smart city ecosystem. In addition, the main algorithms are highlighted, and the advantages/disadvantages are discussed. Most approaches solved two main challenges, which is the scalability and data heterogeneity, offering satisfactory results in comparison to the conventional methods. Other researchers focused on addressing the performance issue, but the tradeoff between aspects such as resources and robustness has compromised some methods.

IV. Discussion, Opportunities and Open Issues

IIoT security concerns have increased exponentially as the risks and sensitivity of data have grown lately. The vulnerabilities in IIoT devices may cause undesirable effects as they are prone to viruses, denial of service attacks, and intrusion attempts. More effective measures should be taken to avoid such situations, hence allowing system developers and IoT device manufacturers to improve their methods for better security [80].

The solutions mentioned above try to solve such issues, but they suffer from some serious security flaws or have many requirements, such as high computation cost or bandwidth. In contrast, others are robust but do not take into account the different characteristics of IIoT devices, such as their limited computational power. Many challenges come from the fact that IIoT systems are complex and can differ significantly from each other, which compromises some security aspects [68].

In a glance, these proposals might be robust and can be applied to various scenarios, including resource-constrained devices. However, they all have their advantages and drawbacks, none of which satisfies all the features. The most notable characteristic that most applications try to achieve is heterogeneity, usually coming at the cost of more computational power [9]. Another strong characteristic is scalability using new technologies such as Blockchain, but most proposals show a tradeoff between communication latency and response delay [84].

In networking and communication, to deal with the granularity (i.e., level of detail in a dataset) of Software Defined Networking (SDN) and NFV-based protection is still an open challenge by considering the inherent tradeoff among performance, flexibility, and cost. The trend nowadays is for interaction among all network architectures layers supporting intrusion detection systems, conversely to the previous focus on the lowest layer level [80]. Many applications also use DL in a centralized and cloud-based server to process all data, hence transferring heavy payloads. However, data processing on edge devices is still an issue in most cases.

The complex environment of IIoT also presents a significant security challenge, yet few methods are capable of satisfying all characteristics ranging from scalability to reliability. Blockchain has enormous potential, and Choo et al. [73] described areas of its use with IIoT, 5G, edge and cloud computing, and trust management. Besides, vulnerability identification and exploitation of Blockchain and IIoT are some key points to promote a secure environment. 5G is becoming a standard as new devices and chips are coming to be compatible with it. Thus, a focus on such technology can improve and solve many issues such as delay and response times, as Luong et al. [55] showed their comparisons of communications between devices.

Muhammad et al. [63] provided a reference model in DL techniques, security, and the smart city paradigm. The combination of its aggregation and the summarizing capabilities of its deep CNN shows promising mechanics for future implementations. The tradeoff between the quality and the processing time should be analyzed together with technologies such as Blockchain to enable a more scalable application.

Table II summarizes contributions as well as the overall advantages and disadvantages.

V. Conclusions and Future Trends

Applications will tend to use more sensitive data as the interest in IIoT grows. As such, to ensure their security is a priority. As an emerging technology, DL is one of the many tools available that enable great results to problems faced in the smart city environment. To this end, we review various studies and deployments of DL in IIoT infrastructure, application, and services and highlight lessons learned.

It is shown that DL is a powerful tool to develop and enable more privacy, security, and efficiency in all fields of smart cities, hence enabling great feats that, otherwise, would be impractical or impossible. Nevertheless, there are more challenges to be faced. Since, by nature, IIoT is a heterogeneous environment, there are still many challenges in defining new protocols, authentication methods as well as to keep privacy awareness at the same time. Resource-constrained devices still have trouble performing more complex tasks as malware detection. Blockchain is another big promising technology that has solved some critical problems regarding scalability

TABLE I
Deep Learning techniques for Industrial IoT

Topic	Publication	Applications	Model	Technique	Function Approximation	Scalability	Reliability	Resource Constrained Devices
Resource Management	[54]	Network	DRL	Service Function Chain (SFC)	Regression	✓	✗	✓
	[55]	Network	DRL	SFC	Regression	✓	✗	✓
	[43]	Device	ANN	Forward Central Dynamic and Available	Regression	✗	✓	✗
Authentication Systems	[8]	Device	DNN	Radio Frequency Physical unclonable functions (RF-PUF)	Classification	✗	✓	✗
	[11]	Device	DRL	Game Theory, Nash Equilibrium, LSTM	Classification	✓	✓	✓
	[59]	Device	RNN	SVM, LSTM	Classification	✓	✗	✓
	[36]	Device	DNN	SVM, LSTM	Regression	✓	✓	✗
Surveillance	[62]	Software	DNN	Bi-directional Long Short-term Memory	Classification	✓	✗	✗
	[3]	Software	CNN	LSTM	Classification	✗	✓	✓
	[63]	Software	CNN	Hierarchal Weighted Fusion	Classification	✗	✓	✓
	[64]	Software	DNN	Hierarchal Weighted Fusion	Classification	✗	✓	✓
	[38]	Network	CNN	Siamese U-Nets and Semantic Segmentation	Regression	✗	✓	✗
	[37]	Software	DNN	Two-path information propagation and stage-wise network refinement	Classification	✗	✓	✗
Privacy Awareness	[70]	Software	CNN & DRL	Markov Decision Process	Classification	✓	✓	✗
	[69]	Network	DNN	Post-Decision State Algorithm	Regression	✗	✓	✗
	[7]	Network	DNN	Proxy Re-Encryption	Regression	✓	✗	✗
Attacks and Threads Detection	[78]	Network	DNN & CNN	Term Frequency and Inverse Document Frequency and Logarithm of Term Frequency weighting techniques	Regression	✗	✓	✗
	[79]	Device	DEL	Operational Code Sequence	Classification	✓	✗	✓
	[12]	Device	DNN	Statistical Signal Processing	Classification	✓	✗	✗
	[41]	Device	CNN	LSTM	Classification	✗	✓	✓
	[81]	Network	DNN	Deep-Feature Extraction and Selection	Classification	✓	✗	✗
	[32]	Device	CNN	Dual Disaggregation and Aggregation DL models	Regression	✗	✗	✓
	[13]	Software	DDL	Multiple Concurrent Models	Classification	✓	✗	✗
	[45]	Software	CNN	Feature Selection and Grey Wolf Optimization.	Regression	✓	✓	✗

and security because of its capability to offer transparency and integrity properties. However, it is still yet to mature for consistency method and delay response.

DL has solved many problems in IIoT applications enabling for a more secure environment and can be refined to provide even better solutions. We envision that the outcome will facilitate future research efforts in spreading new methods. This work aims to be an introductory guide regarding IIoT security in smart cities for students and professionals in the industry, and a reference model for senior researchers.

References

[1] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for iot security based on learning techniques," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019.

[2] B. Yin, H. Yin, Y. Wu, and Z. Jiang, "Fdc: A secure federated deep learning mechanism for data collaborations in the internet of things," *IEEE Internet of Things Journal*, 2020.

[3] T. Hussain, K. Muhammad, J. Del Ser, S. W. Baik, and V. H. C. de Albuquerque, "Intelligent embedded vision for summarization of multi-view videos in iiot," *IEEE Transactions on Industrial Informatics*, 2019.

[4] M. A. Santos, R. Munoz, R. Olivares, P. P. Rebouças Filho, J. Del Ser, and V. H. C. de Albuquerque, "Online heart monitoring systems on the internet of health things environments: A survey, a reference model and an outlook," *Information Fusion*, vol. 53, pp. 222–239, 2020.

[5] T. Alladi, V. Chamola, B. Sikdar, and K. R. Choo, "Consumer iot: Security vulnerability case studies and solutions," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 17–25, 2020.

[6] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying iot security: an exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[7] X. Zhang, X. Chen, J. Liu, and Y. Xiang, "Deeppar and deepdpa: Privacy-preserving and asynchronous deep learning for industrial iot," *IEEE Transactions on Industrial Informatics*, 2019.

[8] B. Chatterjee, D. Das, S. Maity, and S. Sen, "Rf-puf: Enhancing iot security through authentication of wireless nodes using in-situ machine learning," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 388–398, 2018.

[9] L. Oliveira, J. J. Rodrigues, S. A. Kozlov, R. A. Rabêlo, and V. H. C. d. Albuquerque, "Mac layer protocols for internet of things: A survey," *Future Internet*, vol. 11, no. 1, p. 16, 2019.

[10] M. E. Khoda, T. Imam, J. Kamruzzaman, I. Gondal, and A. Rahman, "Robust malware defense in industrial iot applications using machine learning with selective adversarial samples," *IEEE Transactions on Industry Applications*, 2019.

[11] A. Ferdowsi and W. Saad, "Deep learning for signal authentication and security in massive internet-of-things systems," *IEEE Transactions on*

TABLE II
SUMMARIZED DEEP LEARNING TECHNIQUES FOR SECURITY IIOT

Topic	Publication	Advantages	Disadvantages
Resource Management	[54]	Small delay even when using medium numbers of SFC's and MEC enablers for Blockchain	Since it uses MEC and SFC, it cannot be reliable
	[55]	Shows good response in scalability and considerable small processing	Cannot guaranty reliability
	[43]	Significant energy saving in the communication of data transmission by controlling duty cycle in acceptable reliability	There is a greater complexity in implementing the method and it offers a significant communication delay
Authentication Systems	[8]	Very reliable and low error rate	There is a tradeoff between the robustness and security depending on the application
	[11]	Greatly increase its authentication rate as the number of devices is the target	If the number of targets is too low it can have a low rate of successes
	[59]	High accuracy and can be applied to a highly resource-limited device	Too dependent on the training of the RNN
	[36]	High accuracy and fast training with data augmentation	Can be resource demanding
Surveillance	[62]	High accuracy even with low quality and unstable image	High computational cost and not suitable for local processing
	[3]	Low computational power, capable of running in a local device	Cannot detect the anomalous behavior and lacks smoke and fire detection
	[63]	Appropriate for both static and dynamic salience computation	No sequence learning mechanism
	[64]	Low computational power and refined for industrial area	Not suitable for multi-view, lacking in quantity and number of views
	[38]	Multi-resolution ability and tolerance to noise	Limited to the petroleum and gas environment
	[37]	Capable of processing in different angles and distances as well as to detect multiple objects	It is necessary to prepare and have some information about the data before the training, such as the size and any invalid data
Privacy Awareness	[70]	Small error rate in large number of devices	Bad tradeoff between time and accuracy as it scales to quickly
	[69]	Significant speed training for IoT devices and a good tradeoff between privacy and utility	Can be significant slower depending on the number of neurons used
	[7]	Lightweight and effective for a limited numbers of devices	Considerable overhead in the devices in small numbers
Attacks and Threads Detection	[78]	Combines the strength of two DL techniques to increase data classification rate	Since it uses image processing, it can be computationally demanding and lacks scalability for the same reason
	[79]	High accuracy in classification of code	Limited test and not suitable to be applied in large networks
	[12]	Scalable and heterogeneous environment	Too basic comparisons and no performance evaluation presented
	[41]	Scalable and can be applied in a very heterogeneous environment	Still struggles for devices with delay-sensitive
	[81]	High accuracy in classification of attacks and runs in a heterogeneous environment	Limited to impersonation attack and not suitable for resource-constrained devices
	[32]	Fast detection and classification of attacks	Limited to physical interactions of devices
	[13]	Deployable in heterogeneous devices and several completely different models for higher accuracy	High computational cost for edge devices
	[45]	Real-time response in cloud environment with high accuracy	Lacks a malware detection and does not comprehend the heterogeneity of the environment

Communications, vol. 67, no. 2, pp. 1371–1387, 2018.

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

[13] Z. Tian, C. Luo, J. Qiu, X. Du, and M. Guizani, "A distributed deep learning system for web attack detection on edge devices," *IEEE Transactions on Industrial Informatics*, 2019.

[14] T. Alladi, V. Chamola, and S. Zeadally, "Industrial control systems: Cyberattack trends and countermeasures," *Computer Communications*, vol. 155, pp. 1 – 8, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366419319991

[15] C. Esposito, X. Su, S. A. Aljawarneh, and C. Choi, "Securing collaborative deep learning in industrial applications within adversarial scenarios," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4972–4981, 2018.

[16] K. Muhammad, S. Khan, M. Elhoseny, S. H. Ahmed, and S. W. Baik, "Efficient fire detection for uncertain surveillance environment," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 5, pp. 3113–3122, 2019.

[17] A. Ullah, K. Muhammad, I. U. Haq, and S. W. Baik, "Action recognition using optimized deep autoencoder and cnn for surveillance data streams of non-stationary environments," *Future Generation Computer Systems*, vol. 96, pp. 386–397, 2019.

[18] I. Mehmood, A. Ullah, K. Muhammad, D.-J. Deng, W. Meng, F. Al-Turjman, M. Sajjad, and V. H. C. De Albuquerque, "Efficient image recognition and retrieval on iot-assisted energy-constrained platforms from big data repositories," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9246–9255, 2019.

[19] P. Gomes, N. Magaia, and N. Neves, "Industrial and Artificial Internet of Things with Augmented Reality," in *Convergence of Artificial Intelligence and the Internet of Things*. Springer, Cham, 2020, pp. 323–346.

[20] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[21] F. Li, A. Shinde, Y. Shi, J. Ye, X.-Y. Li, and W. Song, "System statistics learning-based iot security: Feasibility and suitability," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6396–6403, 2019.

[22] K. Muhammad, J. J. Rodrigues, S. Kozlov, F. Piccialli, and V. H. C. de Albuquerque, "Energy-efficient monitoring of fire scenes for intelligent networks," *IEEE Network*, vol. 34, no. 3, pp. 108–115, 2020.

[23] T. Hussain, K. Muhammad, W. Ding, J. Lloret, S. Baik, and V. Albuquerque, "A comprehensive survey on multi-view video summarization," *Pattern Recognition*, p. 107567, 07 2020.

[24] W. Ding, M. Abdel-Basset, K. A. Eldrandaly, L. Abdel-Fatah, and V. H. C. de Albuquerque, "Smart supervision of cardiomyopathy based on fuzzy harris hawks optimizer and wearable sensing data optimization: A new model," *IEEE Transactions on Cybernetics*, pp. 1–15, 2020.

[25] K. Muhammad, T. Hussain, J. Rodrigues, P. Bellavista, A. Roberto, and V. Albuquerque, "Efficient and privacy preserving video transmission in 5g-enabled iot surveillance networks: Current challenges and future directions," *IEEE Network*, 06 2020.

[26] M. A. da Cruz, J. J. P. Rodrigues, J. Al-Muhtadi, V. V. Korotaev, and V. H. C. de Albuquerque, "A reference model for internet of things middleware," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 871–883, 2018.

[27] S. Pirbhulal, W. Wu, K. Muhammad, I. Mehmood, G. Li, and V. H. C. de Albuquerque, "Mobility enabled security for optimizing iot based intelligent applications," *IEEE Network*, vol. 34, no. 2, pp. 72–77, 2020.

[28] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, M. Guizani, and A. Al-Fuqaha, "Smart cities: A survey on data management, security, and enabling technologies," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2456–2501, 2017.

[29] H. Yao, P. Gao, J. Wang, P. Zhang, C. Jiang, and Z. Han, "Capsule network assisted iot traffic classification mechanism for smart cities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7515–7525, 2019.

[30] A. Mehra, M. Mandal, P. Narang, and V. Chamola, "Reviewnet: A fast and resource optimized network for enabling safe autonomous driving in hazy weather conditions," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–11, 2020.

[31] T. Han, K. Muhammad, T. Hussain, J. Lloret, and S. W. Baik, "An efficient deep learning framework for intelligent energy management in iot networks," *IEEE Internet of Things Journal*, 2020.

[32] F. Li, Y. Shi, A. Shinde, J. Ye, and W. Song, "Enhanced cyber-physical security in internet of things through energy auditing," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5224–5231, 2019.

[33] C. M. J. M. Dourado, S. P. P. Da Silva, R. V. M. Da Nóbrega, P. P. R. Filho, K. Muhammad, and V. H. C. De Albuquerque, "An open ioht-based deep learning framework for online medical image recognition," *IEEE Journal on Selected Areas in Communications*, pp. 1–1, 2020.

[34] A. Ullah, K. Muhammad, J. Del Ser, S. W. Baik, and V. H. C. de Albuquerque, "Activity recognition using temporal optical flow convolutional features and multilayer lstm," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 12, pp. 9692–9702, 2018.

[35] L. Kong, X.-Y. Liu, H. Sheng, P. Zeng, and G. Chen, "Federated tensor mining for secure industrial internet of things," *IEEE Transactions on Industrial Informatics*, 2019.

[36] R.-F. Liao, H. Wen, S. Chen, F. Xie, F. Pan, J. Tang, and H. Song, "Multi-user physical layer authentication in internet of things with data augmentation," *IEEE Internet of Things Journal*, 2019.

[37] Z. Gao, C. Xu, H. Zhang, S. Li, and V. H. C. de Albuquerque, "Trustful internet of surveillance things based on deeply-represented visual co-saliency detection," *IEEE Internet of Things Journal*, 2020.

[38] M. Santana, L. Passos, T. Moreira, D. Colombo, V. H. C. De Albuquerque, and J. Papa, "A novel siamese-based approach for scene change detection with applications to obstructed routes in hazardous environments," *IEEE Intelligent Systems*, 2019.

[39] J. Zhang, R. S. Blum, and H. V. Poor, "Approaches to secure inference in the internet of things: Performance bounds, algorithms, and effective attacks on iot sensor networks," *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 50–63, 2018.

[40] T. Alladi, V. Chamola, R. M. Parizi, and K. R. Choo, "Blockchain applications for industry 4.0 and industrial iot: A review," *IEEE Access*, vol. 7, pp. 176 935–176 951, 2019.

[41] A. Diro and N. Chilamkurti, "Leveraging lstm networks for attack detection in fog-to-things communications," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 124–130, 2018.

[42] E. Fernandes, A. Rahmati, K. Eykholt, A. Prakash *et al.*, "Internet of things security research," *Looking for the BEST Tech Job for You?*, p. 15, 2019.

[43] A. H. Sodhro, S. Pirbhulal, and V. H. C. de Albuquerque, "Artificial intelligence-driven mechanism for edge computing-based industrial applications," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4235–4243, 2019.

[44] E. Benkhelifa, T. Welsh, and W. Hamouda, "A critical review of practices and challenges in intrusion detection systems for iot: Toward universal and resilient systems," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3496–3509, 2018.

[45] S. Garg, K. Kaur, N. Kumar, G. Kaddoum, A. Y. Zomaya, and R. Ranjan, "A hybrid deep learning-based model for anomaly detection in cloud datacenter networks," *IEEE Transactions on Network and Service Management*, vol. 16, no. 3, pp. 924–935, 2019.

[46] M. Qiu, H.-N. Dai, A. K. Sangaiah, K. Liang, and X. Zheng, "Guest editorial: Special section on" emerging privacy and security issues brought by artificial intelligence in industrial informatics"," *IEEE Transactions on Industrial Informatics*, 2019.

[47] H. Tschofenig and E. Baccelli, "Cyberphysical security for the masses: A survey of the internet protocol suite for internet of things security," *IEEE Security & Privacy*, vol. 17, no. 5, pp. 47–57, 2019.

[48] Y. Zhang, V. Krishnan, J. Pi, K. Kaur, A. Srivastava, A. Hahn, and S. Suresh, "Cyber physical security analytics for transactive energy systems," *IEEE Transactions on Smart Grid*, 2019.

[49] Z. Zhou, K. Chen, and J. Zhang, "Efficient 3-d scene prefetching from learning user access patterns," *IEEE Transactions on Multimedia*, vol. 17, no. 7, pp. 1081–1095, 2015.

[50] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled data collection and sharing for industrial iot with deep reinforcement learning," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3516–3526, 2018.

[51] V. Hassija, V. Chamola, V. Gupta, S. Jain, and N. Guizani, "A survey on supply chain security: Application areas, security threats, and solution architectures," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[52] H. Alasmary, A. Khormali, A. Anwar, J. Park, J. Choi, A. Abusnaina, A. Awad, D. Nyang, and A. Mohaisen, "Analyzing and detecting emerging internet of things malware: a graph-based approach," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8977–8988, 2019.

[53] Z. B. Celik, P. McDaniel, G. Tan, L. Babun, and A. S. Uluagac, "Verifying internet of things safety and security in physical spaces," *IEEE Security & Privacy*, vol. 17, no. 5, pp. 30–37, 2019.

[54] S. Guo, Y. Dai, S. Xu, X. Qiu, and F. Qi, "Trusted cloud-edge network resource management: Drl-driven service function chain orchestration for iot," *IEEE Internet of Things Journal*, 2019.

[55] N. C. Luong, D. T. Hoang, S. Gong, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, "Applications of deep reinforcement learning in communications and networking: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3133–3174, 2019.

[56] F. Hussain, S. A. Hassan, R. Hussain, and E. Hossain, "Machine learning for resource management in cellular and iot networks: Potentials, current solutions, and open challenges," *IEEE Communications Surveys & Tutorials*, 2020.

[57] H. Lu, Y. Zhang, Y. Li, C. Jiang, and H. Abbas, "User-oriented virtual mobile network resource management for vehicle communications," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–12, 2020.

[58] S. Khan Tayyaba, H. A. Khattak, A. Almogren, M. A. Shah, I. Ud Din, I. Alkhalifa, and M. Guizani, "5g vehicular network resource management for improving radio access through machine learning," *IEEE Access*, vol. 8, pp. 6792–6800, 2020.

[59] J. Chauhan, S. Seneviratne, Y. Hu, A. Misra, A. Seneviratne, and Y. Lee, "Breathing-based authentication on resource-constrained iot devices using recurrent neural networks," *Computer*, vol. 51, no. 5, pp. 60–67, 2018.

[60] Z. Gao, H. Zhang, S. Dong, S. Sun, X. Wang, G. Yang, W. Wu, S. Li, and V. H. C. de Albuquerque, "Salient object detection in the distributed cloud-edge intelligent network," *IEEE Network*, vol. 34, no. 2, pp. 216–224, 2020.

[61] J. Zhang, C. Xu, Z. Gao, J. J. P. C. Rodrigues, and V. Albuquerque, "Industrial pervasive edge computing-based intelligence iot for surveillance saliency detection," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2020.

[62] T. Hussain, K. Muhammad, A. Ullah, Z. Cao, S. W. Baik, and V. H. C. de Albuquerque, "Cloud-assisted multiview video summarization using cnn and bidirectional lstm," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 77–86, 2019.

[63] K. Muhammad, T. Hussain, M. Tanveer, G. Sannino, and V. H. C. de Albuquerque, "Cost-effective video summarization using deep cnn with hierarchical weighted fusion for iot surveillance networks," *IEEE Internet of Things Journal*, 2019.

[64] K. Muhammad, H. Tanveer, J. Del Ser, V. Palade, and V. H. C. De Albuquerque, "Deepres: A deep learning-based video summarization strategy for resource-constrained industrial surveillance scenarios," *IEEE Transactions on Industrial Informatics*, 2019.

[65] K. Muhammad, S. Khan, V. Palade, I. Mehmood, and V. H. C. De Albuquerque, "Edge intelligence-assisted smoke detection in foggy surveillance environments," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1067–1075, 2019.

[66] S. Khan, K. Muhammad, S. Mumtaz, S. W. Baik, and V. H. C. de Albuquerque, "Energy-efficient deep cnn for smoke detection in foggy iot environment," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9237–9245, 2019.

[67] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, and F. Titouna, "A privacy-preserving cryptosystem for iot e-healthcare," *Information Sciences*, vol. 527, pp. 493–510, 2020.

[68] R. Chow, "The last mile for iot privacy," *IEEE Security & Privacy*, vol. 15, no. 6, pp. 73–76, 2017.

[69] X. He, R. Jin, and H. Dai, "Deep pds-learning for privacy-aware offloading in mec-enabled iot," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4547–4555, 2018.

[70] Y. Liu, H. Wang, M. Peng, J. Guan, J. Xu, and Y. Wang, "Deepga: A privacy-preserving data aggregation game in crowdsensing via deep reinforcement learning," *IEEE Internet of Things Journal*, 2019.

[71] N. Magaia, C. Borrego, P. Pereira, and M. Correia, "Privo: A privacy-preserving opportunistic routing protocol for delay tolerant networks." IEEE, 6 2017, pp. 1–9.

[72] N. Magaia, C. Borrego, P. R. Pereira, and M. Correia, "eprivo: An enhanced privacy-preserving opportunistic routing protocol for vehicular delay-tolerant networks," *IEEE Transactions on Vehicular Technology*, vol. 67, pp. 11 154–11 168, 11 2018.

[73] K.-K. R. Choo, Z. Yan, and W. Meng, "Blockchain in industrial iot applications: Security and privacy advances, challenges and opportunities," *IEEE Transactions on Industrial Informatics*, 2020.

[74] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial iot," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177–4186, 2020.

[75] Y. Zhao, J. Zhao, L. Jiang, R. Tan, D. Niyato, Z. Li, L. Lyu, and Y. Liu, "Privacy-preserving blockchain-based federated learning for iot devices," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[76] L. Yin, X. Luo, C. Zhu, L. Wang, Z. Xu, and H. Lu, "Connspoiler: Disrupting c&c communication of iot-based botnet through fast detection of anomalous domain queries," *IEEE Transactions on Industrial Informatics*, 2019.

[77] R. R. Guimaraes, L. A. Passos, R. Holanda Filho, V. H. C. de Albuquerque, J. J. Rodrigues, M. M. Komarov, and J. P. Papa, "Intelligent network security monitoring based on optimum-path forest clustering," *Ieee Network*, vol. 33, no. 2, pp. 126–131, 2018.

[78] F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M. A. Latif, F. Al-Turjman, and L. Mostarda, "Cyber security threats detection in internet of things using deep learning approach," *IEEE Access*, vol. 7, pp. 124 379–124 389, 2019.

[79] A. Azmoodeh, A. Dehghantanha, and K.-K. R. Choo, "Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning," *IEEE Transactions on Sustainable Computing*, vol. 4, no. 1, pp. 88–95, 2018.

[80] K. A. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of things: A survey on machine learning-based intrusion detection approaches," *Computer Networks*, vol. 151, pp. 147–157, 2019.

[81] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, "Deep abstraction and weighted feature selection for wi-fi impersonation detection," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 621–636, 2017.

[82] N. Magaia, P. Pereira, and M. Correia, "REPSYS: A Robust and Distributed Reputation System for Delay-Tolerant Networks," in *Proceedings of the 20th ACM International Conference on Modelling, Analysis and Simulation of Wireless and Mobile Systems - MSWiM '17*. New York, New York, USA: ACM Press, 2017, pp. 289–293.

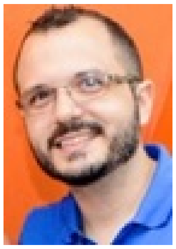
[83] N. Magaia and Z. Sheng, "ReFIoV: A novel reputation framework for information-centric vehicular applications," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1810–1823, 2019.

[84] A. Barki, A. Bouabdallah, S. Gharout, and J. Traore, "M2m security: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1241–1254, 2016.

Naercio Magaia received his Ph.D. in Electrical and Computer Engineering from Instituto Superior Técnico (IST), University of Lisbon (ULisboa). He holds a degree in Electrical Engineering from Eduardo Mondlane University, and an M.Sc. in Communication Networks Engineering from IST, ULisboa. He is currently an Invited Assistant Professor at the Faculty of Sciences of ULisboa and an integrated researcher at the LASIGE research unit. His current research interests cover Computer Networks, Network Security, and Artificial Intelligence.

Ramon Fonseca is graduated in Control and Automation Engineering and undergraduate in Computer Engineering at the University of Fortaleza (UNIFOR). His research interests include Computer Vision, ML, Robotics and Motion Control.

Khan Muhammad [S'16, M'18] received the Ph.D. degree in digital contents from Sejong University, Seoul, South Korea. He is currently an Assistant Professor with the Department of Software, Sejong University. He has registered more than ten patents and authored or co-authored more than 140 papers in peer reviewed international journals and conferences in his areas of research. He is also serving as a Professional Reviewer for over 100 well-reputed journals and conferences. His research interests include medical image analysis (brain MRI, diagnostic hysteroscopy and wireless capsule endoscopy), information security (steganography, encryption, watermarking and image hashing), video summarization, computer vision, fire/smoke scene analysis, and video surveillance. He is also Editorial Board Member of "Journal of Artificial Intelligence and Systems" and "Mathematics of Computation and Data Science".



Afonso H. Fontes N. Segundo Control and Automation Engineer with an emphasis in Robotics. Master of Science in Computer Science in artificial intelligence and software development. Lecturer in Robotics, Autonomous Systems, and Digital Control. Afonso is a member of the Computer Systems research group hosted by the Ph.D. program on Applied Informatics at UNIFOR and a Ph.D. student at the Department of Computer Science and Engineering at Chalmers and the University of Gothenburg.

Aloísio Vieira Lira Neto is the Superintendent of the Superintendence of Research and Strategy for Public Safety of Ceará and a Special Agent of Federal Highway Police. He graduated in Public Safety Management from the University of Southern Santa Catarina. He is currently a Master's student in Applied Informatics at the University of Fortaleza (UNIFOR). He has experience in Strategic Intelligence, Intelligent Systems, Pattern Recognition, Artificial Intelligence, and Sociology, with emphasis on Violence, Criminality, and Police Action.

Victor Hugo C. de Albuquerque [M'17, SM'19] is a professor and senior researcher at the LAPISCO/IFCE, and ARMTEC Tecnologia em Robótica, Brazil. He has a Ph.D in Mechanical Engineering from the Federal University of Paraíba (UFPB, 2010), an MSc in Teleinformatics Engineering from the Federal University of Ceará (UFC, 2007), and he graduated in Mechatronics Engineering at the Federal Center of Technological Education of Ceará (CEFETCE, 2006). He is a specialist, mainly, in IoT, Machine/Deep Learning, Pattern Recognition, Robotic.