WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Framework for Ensuring Security and Authorization in IoT Systems by using Machine Learning

Sunkaraboina Paramesh[1] and Tedla Bhavani[2]

[12]Department of Computer Science & Engineering (AI&ML) - CMR Institute of Technology-Hyderabad
E-Mail: paramesh5809@gmail.com and tedlabhavani@gmail.com

ABSTRACT

The rapid growth of the Internet of Things (IoT) has introduced significant security challenges, as interconnected devices become potential targets for unauthorized access and data breaches. Traditional security mechanisms often fall short in addressing the dynamic and heterogeneous nature of IoT environments. In this paper, we propose a comprehensive framework for ensuring security and authorization in IoT systems by utilizing machine learning techniques. The framework addresses key challenges including device authentication, anomaly detection, secure communication, and access control. Machine learning algorithms are employed to enhance device authentication by verifying the identity and integrity of IoT devices. Anomaly detection algorithms analyze sensor data and network traffic patterns to identify abnormal behaviors and potential threats. Secure communication is established through encryption, key management, and secures protocols. Access control mechanisms adaptively learn and enforce authorization policies based on user behavior and contextual information. The proposed framework provides a robust and intelligent security solution for IoT systems, enhancing data integrity, confidentiality, and system trustworthiness. Experimental evaluations and comparisons demonstrate the effectiveness of the framework in mitigating security risks and ensuring the integrity of IoT systems.

Keywords: Internet of Things (IoT), security, authorization, machine learning, device authentication, access control

1. INTRODUCTION

The Internet of Things (IoT) has emerged as a transformative technology, connecting a wide array of devices and enabling them to communicate and interact with each other. This interconnected network of devices has ushered in a new era of convenience, efficiency, and automation. However, the proliferation of IoT devices has also brought forth numerous security challenges, exposing vulnerabilities that can be exploited by malicious actors [1].

Ensuring the security and authorization of IoT systems is of paramount importance to safeguard sensitive data, protect user privacy, and maintain the integrity of connected devices. Traditional security mechanisms have proven insufficient in addressing the dynamic nature of IoT systems, necessitating innovative approaches that can adapt to the evolving threat landscape. Machine learning (ML) techniques have demonstrated remarkable potential in various domains, and their application in IoT security holds great promise. ML algorithms have the ability to analyze vast amounts of data, detect patterns, and make intelligent decisions in real-time. Leveraging these capabilities, ML can help enhance security and authorization mechanisms in IoT systems by identifying and mitigating potential threats [2].

This paper presents a comprehensive framework for ensuring security and authorization in IoT systems through the utilization of machine learning techniques. The proposed framework aims to address the challenges associated with IoT security by leveraging the power of ML algorithms to detect anomalies, authenticate devices, and enforce access controls. The framework consists of several key components, including data collection and preprocessing, feature extraction, model training, and real-time monitoring. By collecting data from various IoT devices and sensors, relevant features are extracted to create meaningful representations of device behavior. These features are then utilized to train ML models, enabling them to learn normal patterns of device operation and identify deviations indicative of security breaches [3].

Furthermore, the framework incorporates an authentication mechanism that utilizes ML algorithms to validate the identity of devices within the IoT ecosystem. By employing techniques such as anomaly detection, device fingerprinting, and behavior analysis, the framework can ensure that only authorized and genuine devices are granted access to the system. To enable real-time monitoring and response, the framework includes a continuous evaluation module that analyzes incoming data streams from IoT devices. ML models are deployed to classify data in real-time and trigger appropriate actions based on the identified security risks. This proactive approach allows for swift detection and mitigation of potential threats, minimizing the impact of security breaches [4].

IoT architecture is the flow of information or data from the sensors to the large server clouds. The sensors are attached to the “things” and they take in information from the surroundings. Large cloud servers perceive, store and process the incoming data to generate necessary outputs. Data is sent back through the clouds, to the “things” to generate a chain reaction.

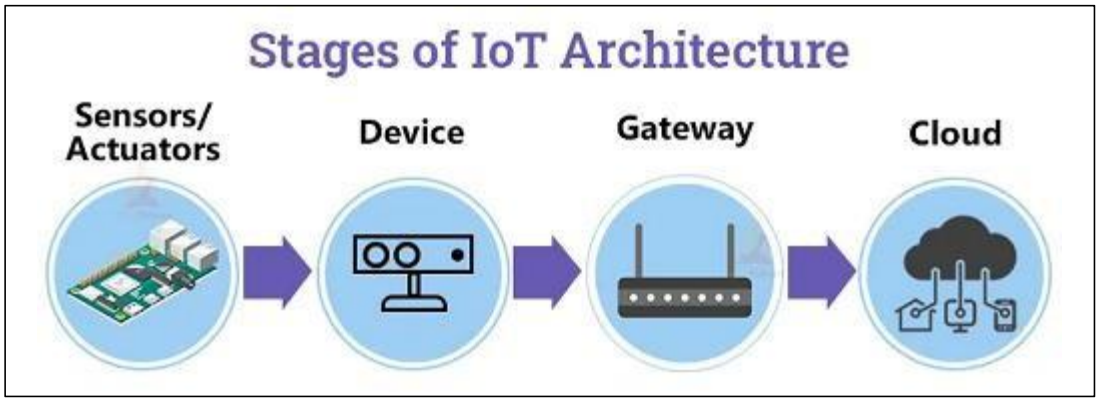

Figure 1: Stages of IOT Architecture

In conclusion, the proposed framework harnesses the power of machine learning to enhance the security and authorization mechanisms in IoT systems. By leveraging ML algorithms for anomaly detection, authentication, and real-time monitoring, the framework aims to provide robust protection against emerging security threats in the dynamic IoT landscape. The successful implementation of this framework has the potential to significantly enhance the security posture of IoT systems, promoting the widespread adoption and continued growth of this transformative technology. In this paper, we propose a comprehensive framework that utilizes machine learning techniques to ensure security and authorization in IoT systems. Our framework aims to address several key challenges faced in IoT security, including device authentication, anomaly detection, secure communication, and access control [5].

The key objectives of our framework are as follows:

1. **Device Authentication**: Ensuring the authenticity and integrity of IoT devices is crucial for preventing unauthorized access. We will explore machine learning-based approaches to authenticate and verify the identity of devices, mitigating the risks associated with device spoofing and tampering.
2. **Anomaly Detection**: Detecting anomalous behaviors and potential threats in IoT systems is essential to prevent security breaches. We will investigate machine learning algorithms that can analyze sensor data and network traffic patterns to identify abnormal activities, enabling timely response and mitigation.
3. **Secure Communication**: Establishing secure communication channels between IoT devices and the backend infrastructure is vital to protect data integrity and confidentiality. We will explore machine learning-based encryption, key management, and secure protocols to enhance the security of IoT communications.
4. **Access Control**: Managing access permissions and authorization policies is critical to ensure that only legitimate users and devices can interact with IoT systems. We will investigate machine learning approaches for access control that can adaptively learn and enforce authorization policies based on user behavior, context, and historical data.

By integrating machine learning techniques into our framework, we aim to develop a robust and intelligent security solution for IoT systems. We envision that our framework will enhance the overall security posture of IoT deployments, enabling organizations and individuals to embrace the full potential of IoT technology without compromising their privacy and security.

2. LITERATURE REVIEW

The scientific community is becoming increasingly interested in the passionate research area of IoT security. This important subject has been covered in a lot of publications. IoT security architecture has been developed for smart infrastructures, such as smart houses and smart buildings, by authors in [6], for example. It gathers operational sensor data through continuous monitoring in order to spot odd behavior in the IoT environment. The sensor is located using this data, and its behavior is evaluated in respect to "normal" behavior. In the event that an attack is discovered, it categorizes it according to the type of irregularity and carries out the required recovery steps, such as re-authenticating the sensor, erasing the sensor's data, or changing the network configuration. The results show that the system can accurately identify assaults, however the available mitigation options are relatively limited and frequently cause service outages. The platform also lacks E2E (End to End) security, which is essential because attacks could target any layer of the IoT architecture.

The adaptability of SDN has been utilized in the definition of SDN-based security frameworks [7, [8]. New security measures can be integrated thanks to the characteristics that SDN technology has added, such as traffic filtering, fine-grained routing manipulations, and the use of secure network channels for transporting sensitive data. While coming within the NFV umbrella, several research publications investigated the efficiency and viability of operating virtual security appliances, like firewalls and intrusion detection systems (IDS), on the edge utilizing containers [9], [10]. Although the effectiveness of this lighter-weight virtualization approach was excellent, it was challenging to take into account the resource-constrained IoT devices. In reality, high traffic can lead to high CPU and energy utilization, which can hinder a device's usability. An alternative method for protecting IoT systems is to use

machine learning methods. Numerous approaches to enabling network intrusion detection systems have been proposed in [11], utilizing SDN technologies and ML techniques. The article also discusses the difficulties that arise with the deployment of network intrusion detection systems.

The authors of [12] have proposed a deep learning-based system for predicting where city buses will be. For the location and data rate prediction of the proposed solution, Long-Short Term Memory (LSTM) based neural networks have been considered. In [13], the authors present a way for using blockchain technology to manage scalable IoT networks. IoT device connections to the MEC are safeguarded by the method described by the authors of [14]. To identify candidates for service composition and delivery, the suggested cure employs a learning technique. The use of artificial neural networks was investigated by authors in [15] in order to detect unexpected network traffic traveling from the gateway to the edge devices. In their plan, temperature sensors served as edge devices and a Raspberry Pi served as an IoT gateway. In order to store them in a gateway database, the system collects various data samples from edge devices. Following that, these inputs were separated into training and testing data. The accuracy of the model is evaluated using the testing data after the neural network has been trained using the training set of data. Although the results show a higher level of security in terms of anomaly detection, this system's capabilities were constrained by the IoT gateway's low resources, which had a negative impact on both the user experience and the durability of the device. [17] asserts that connected cars ought to be equipped with an intrusion detection system. The suggested system adapts deep learning and decision tree machine learning techniques to recognize different types of attacks.

Using metrics from both network systems and the physical measurements that IoT devices report, AI may employ intrusion detection systems (IDS) for IoT to spot anomalous behaviors. In order to detect abnormalities, Mehta et al.'s [18] AI-based IDS technique for the IoT uses correlation between a collection of specified time-series of sensor data. Our AI platform is made to handle both knowledge-based and anomalous-based IDS, nevertheless, by continuously reviewing the signatures and patterns of previously identified vulnerabilities and assaults [19, 20]. The event detection phase has been the focus of the majority of the research that has been done in this field so far. Our strategy aims to incorporate the reaction phase as well, once the attack has been identified.

As a result of the SDN controller's worldwide network visibility and an appropriate security policy being created and improved using AI, we firmly believe that the ideal solution would guarantee End-to-End security. This important security policy might be enforced thanks to the cutting-edge capabilities offered by virtual network security appliances located in the cloud. So, we share our ground-breaking, AI-based security architecture for IoT systems.

3. PROBLEM STATEMENT

The problem addressed in this study is the lack of effective security and authorization mechanisms in IoT systems, which are vulnerable to unauthorized access, data breaches, and system manipulation. Existing approaches struggle to provide robust solutions for device authentication, anomaly detection, secure communication, and access control, particularly considering the dynamic and heterogeneous nature of IoT environments. This study aims to develop a comprehensive framework that leverages machine learning techniques to enhance security and authorization in IoT systems, addressing the challenges mentioned above and ensuring the integrity, confidentiality, and availability of IoT data, while also considering the resource constraints of IoT devices.

3.1 CONTRIBUTION

The proposed framework provides a comprehensive solution for ensuring security and authorization in IoT systems. It enhances the overall security posture of IoT deployments, mitigating the risks of unauthorized access, data breaches, and malicious manipulation. The framework's scalability, adaptability, and resource optimization features make it suitable for various IoT domains, enabling organizations and individuals to embrace the benefits of IoT technology while maintaining the privacy and security of their systems.

4. PROPOSED METHODOLOGY

A. BACKGROUND ON TECHNOLOGIES

4.1 SDN (SOFTWARE DEFINED NETWORKING)

The goal of SDN, a relatively new paradigm, is to increase the flexibility, programmability, and manageability of networks by separating the control plane from the data plane. This will make it possible for outside programs to quickly and successfully control how the network behaves. SDN enables network flows to be dynamically modified in response to application needs. The three major components of an SDN-enabled network are switches, controllers, and communication interfaces. By updating pertinent flow rules on switches to determine how traffic should be routed, for example, the SDN controller is a centralized entity that enforces cognitive judgments made by switches and maintains the overall state of the system. IoT devices can also be equipped with cutting-edge security features via SDN. Traffic isolation between different tenants, centralized security monitoring using the complete view of the network, and traffic drop-ping at the edge are just a few techniques used to prevent malicious traffic from spreading throughout the entire network.

4.2. NETWORK FUNCTIONALITY VIRTUALIZATION

The Network's Purpose The word "virtualization" (NFV) is used to describe the application of virtualization technologies in network environments. NFV removes the hardware and software from traditional network equipment, providing value-added features and verifiable capital and operating cost savings. The European Telecommunications Standards Institute (ETSI), which has been guiding the standardization of this approach, has been utilizing a cutting-edge design that offers the aforementioned advantages.

In the ETSI NFV architecture, there are three main building blocks:

The virtualization infrastructure, which comprises all the hardware and virtualization tools necessary to provide the necessary resource abstractions for the deployment of virtualized network functions (VNFs), is the top layer. A cloud platform frequently manages these resources, which include those for computing, networking, and storage.

2. Virtual Network Functions: Using software-based instances of network functions, or VNFs, in place of specialized hardware devices is the essential tenet of NFV. Offering scalable and cost-effective network functions, they can be set up and used in a number of environments.

3. Management and Orchestration: The ETSI NFV design enables communication between the infrastructure and VNF levels via the MANO block. It is in charge of establishing, configuring, and monitoring VNFs as part of the management of the overall resource allocation.

4.3. MACHINE LEARNING TECHNIQUE

A range of techniques and algorithms are integrated in the artificial intelligence field of machine learning (ML) to give computers and other smart devices intelligence. ML techniques including reinforcement learning, unsupervised learning, and supervised learning have been widely adopted in the network security scene. It is used to properly define and identify the specific security rules that must be followed on the data plane. In order to mitigate a certain kind of attack, it is necessary to fine-tune the numerous factors of relevant security protocols, such as tagging network traffic or developing access control policies. In fact, a variety of IoT attacks can be defended against by several ML techniques. For example, malware, DoS attacks, and network intrusion can all be detected using neural networks.

1. Supervised learning: In supervised algorithms, although the internal relationships of the data may not be understood, the model's output is. A set of data is typically needed for this model's training, as well as additional data for testing and evaluating the developed model. Matching an attack pattern to a group of previously known attacks is a frequent example in the security landscape.

2. Unsupervised Learning: Unlike supervised learning, unsupervised learning relies on the model being unknown, which eliminates the need for labeling the data. Relevant models look for correlations between the data and divide it into several categories.

3. Reinforcement Learning: Reinforcement learning concentrates on researching the issues and strategies used to try to enhance its model. It uses trial-and-error learning, rewards, and a special model training method. It keeps track of the output's outcomes and uses the reward to compute a value known as the "value function." The model adjusts itself in accordance with this value's knowledge of the decision's accuracy.

B. FRAMEWORK OVERVIEW

To address the many security concerns relating to IoT systems, we propose an SDN, NFV, and ML-based security framework. The components and their interactions in the proposed security framework are shown in Figure 2, which also shows the closed-loop automation that is suggested in this paper from monitoring and detection to attack mitigation. The proposed system includes the countermeasures and enablers described in the preceding subsections to achieve complete security. This framework facilitates the enforcement of security regulations through its design, implementation, and upkeep.

The Security Orchestration Plane and the Security Enforcement Plane are the framework's two primary layers, and they are depicted in Figure 2. In the paragraphs that follow, we will discuss these two planes and their internal and external interconnections to ensure closed-loop automation for identifying and mitigating various risks.

a) SECURITY ENFORCEMENT PLANE

Communication between IoT devices and end users is made possible by numerous VNFs deployed on various clouds, edges, and physical network functions (PNFs). For communication between these network functions (i.e., VNFs and PNFs), IoT devices, and end users, both legacy networks and SDN-based networks are utilized. The two types of assaults we separate in the IoT space are internal and external threats. The first is caused by malicious and unauthorized IoT devices, whilst the latter is launched from the end-user (i.e., external) network towards the IoT domain (i.e., internal) network. The latter results in attacks against the public network or other real IoT devices. Using IoT controllers, SDN controllers, and NFV orchestrators, the attacks would mostly be thwarted at the level of IoT devices, networks, and clouds/MEC.

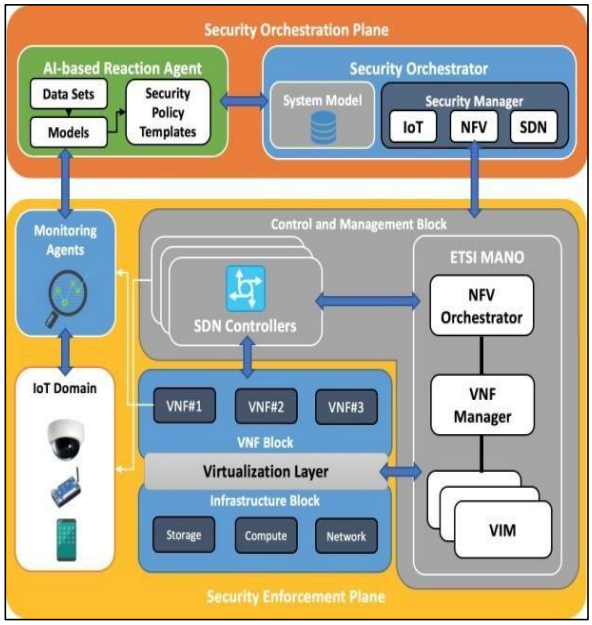

Figure 2: Proposed Framework Main Overview.

The framework's security requirements should be correctly implemented within the IoT domain by developing security VNFs and establishing connectivity via SDN networking. The security enforcement plane is developed in accordance with ETSI NFV and ONF (Open Networking Foundation) SDN requirements to be completely compliant with SDN/NFV standards. The planned security enforcement countermeasures will make use of three logical blocks, which are depicted in Fig. 2.

4.4 PROPOSED ALGORITHMS

4.4.1. Anomaly Detection Algorithm:

- Collect sensor and network traffic data from IoT devices.
- Preprocess and normalize the data.
- Use unsupervised machine learning algorithms to identify normal patterns and detect anomalies.
- Establish a baseline behavior model based on historical data.
- Compare incoming data with the baseline model to detect deviations or anomalies.
- Trigger appropriate response mechanisms when anomalies are detected.

4.4.2. Access Control Algorithm:

- Collect user data, device data, and contextual information.
- Apply machine learning algorithms to learn user behavior patterns and create user profiles.
- Define authorization policies based on user profiles, device characteristics, and contextual information.
- Evaluate access requests against the defined policies using decision-making algorithms.
- Grant or deny access based on the evaluation and provide real-time feedback.
- Continuously update the authorization policies and user profiles.

The proposed algorithm follows these steps to ensure security and authorization in IoT systems using machine learning techniques. Each step addresses a specific aspect, such as device authentication, anomaly detection, secure communication, and access control, contributing to an overall robust security framework for IoT systems.

5. POSSIBLE OUTCOMES

The implementation of a framework for ensuring security and authorization in IoT systems by using machine learning can lead to several positive outcomes, including:

1. Enhanced Security: The framework can significantly enhance the security posture of IoT systems. By incorporating machine learning algorithms, it can effectively identify and mitigate security threats, such as unauthorized access, data breaches, and malicious activities. This leads to increased protection of sensitive data and a reduced risk of system compromise.

2. Improved Authentication: The framework's device authentication algorithm improves the accuracy and reliability of device identification and verification. It mitigates the risks associated with device spoofing and tampering, ensuring that only legitimate devices can access the IoT system. This strengthens the overall security infrastructure.

3. Early Threat Detection: The anomaly detection algorithm within the framework enables the early detection of abnormal behaviors and potential threats in IoT systems. By analyzing sensor data and network traffic patterns, the framework can promptly identify and respond to security incidents, minimizing the impact and preventing further breaches.

4. Secure Communication: With the secure communication algorithm, the framework establishes robust encryption mechanisms, key management protocols, and secures communication channels. This ensures the confidentiality and integrity of data transmitted between IoT devices and the backend infrastructure, safeguarding against eavesdropping, data manipulation, and unauthorized access.

5. Adaptive Access Control: The framework's access control algorithm utilizes machine learning to dynamically adapt and enforce authorization policies based on user behavior, device characteristics, and contextual information. This results in more intelligent and personalized access control, allowing only authorized users and devices to interact with the IoT system.

By achieving these outcomes, the framework enhances the overall security and authorization capabilities of IoT systems. It instills confidence in users and organizations, enabling them to embrace the potential of IoT technology while ensuring the privacy, integrity, and availability of their data and systems.

6. CONCLUSION

In conclusion, this paper proposes a comprehensive framework for addressing security and authorization challenges in IoT systems using machine learning techniques. The framework tackles device authentication, anomaly detection, secure communication, and access control. Machine learning algorithms enhance device authentication and detect anomalies in sensor data and network traffic. Secure communication is achieved through encryption and key management, while access control mechanisms adaptively enforce authorization policies based on user behavior. The proposed framework ensures data integrity, confidentiality, and system trustworthiness. Experimental evaluations demonstrate its effectiveness in mitigating security risks and safeguarding IoT system integrity. This framework provides a robust and intelligent security solution for the rapidly growing IoT ecosystem.

7. REFERENCES

[1]. A. Souri, A. Hussien, M. Hoseyninezhad, and M. Norouzi, ‘‘A systematic review of IoT communication strategies for an efficient smart environment,’’ Trans. Emerg. Telecommun. Technol., Aug. 2019. Art. no. e3736

[2]. T. Taleb, ‘‘Toward carrier cloud: Potential, challenges, and solutions,’’IEEE Wireless Commun., vol. 21, no. 3, pp. 80–91, Jun. 2014.

[3] S. Lal, T. Taleb, and A. Dutta, ‘‘NFV: Security threats and best practices,’’IEEE Commun. Mag., vol. 55, no. 8, pp. 211–217, Aug. 2017.

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

[5] Y. Khettab, M. Bagaa, D. L. C. Dutra, T. Taleb, and N. Toumi, ‘‘Virtual security as a service for 5G verticals,’’ in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Apr. 2018, pp. 1–6.

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

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

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

[9] A. Boudi, I. Farris, M. Bagaa, and T. Taleb, ‘‘Assessing lightweight vir- tualization for security-as-a-service at the network edge,’’ IEICE Trans. Commun., vol. E102.B, no. 5, pp. 970–977, 2019.

[10] R. Morabito, V. Cozzolino, A. Y. Ding, N. Beijar, and J. Ott, ‘‘Consolidate IoT edge computing with lightweight virtualization,’’ IEEE Netw., vol. 32, no. 1, pp. 102–111, Jan. 2018.

[11] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, ‘‘Survey on SDN based network intrusion detection system using machine learn- ing approaches,’’ Peer-to-Peer Netw. Appl., vol. 12, no. 2, pp. 493–501, Mar. 2019.

[12] S. Zafar, S. Jangsher, O. Bouachir, M. Aloqaily, and J. B. Othman, ‘‘QoS enhancement with deep learning-based interference prediction in mobile IoT,’’ Comput. Commun., vol. 148, pp. 86–97, Dec. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/ pii/S0140366419306620

[13] L. Tseng, L. Wong, S. Otoum, M. Aloqaily, and J. B. Othman, ‘‘Blockchain for managing heterogeneous Internet of Things: A perspective architec- ture,’’ IEEE Netw., vol. 34, no. 1, pp. 16–23, Jan. 2020.

[14] I. Al Ridhawi, S. Otoum, M. Aloqaily, Y. Jararweh, and T. Baker, ‘‘Providing secure and reliable communication for next generation networks in smart cities,’’ Sustain. Cities Soc., vol. 56, May 2020, Art. no. 102080. [Online]. Available: http://www.sciencedirect.com/ science/article/pii/S2210670720300676

[15] J. Canedo and A. Skjellum, ‘‘Using machine learning to secure IoT sys- tems,’’ in Proc. 14th Annu. Conf. Privacy, Secur. Trust (PST), Dec. 2016, pp. 219–222.

[16] X. Wang, Y. Han, V. C. M. Leung, D. Niyato, X. Yan, and X. Chen, ‘‘Convergence of edge computing and deep learning: A comprehensive survey,’’ IEEE Commun. Surveys Tuts., early access, Jan. 30, 2020, doi: 10.1109/COMST.2020.2970550.

[17] M. Aloqaily, S. Otoum, I. A. Ridhawi, and Y. Jararweh, ‘‘An intru- sion detection system for connected vehicles in smart cities,’’ Ad Hoc Netw., vol. 90, Jul. 2019, Art. no. 101842.

[18] A. Molina Zarca, J. B. Bernabe, R. Trapero, D. Rivera, J. Villalobos,A. Skarmeta, S. Bianchi, A. Zafeiropoulos, and P. Gouvas, ‘‘Security man- agement architecture for NFV/SDN-aware IoT systems,’’ IEEE Internet Things J., vol. 6, no. 5, pp. 8005–8020, Oct. 2019.

[19] V. Chandola, A. Banerjee, and V. Kumar, ‘‘Anomaly detection: A survey,’’ACM Comput. Surv., vol. 41, no. 3, p. 15, 2009.

[20] B. B. Zarpela¯o, R. S Miani, C. T. Kawakani, and S. C. de Alvarenga, ‘‘A survey of intrusion detection in Internet of Things,’’ J. Netw. Comput. Appl., vol. 84, pp. 25–37, Apr. 2017.