Modelling Decision and Reaction against Detected Intrusions in IoT System basing on security policy rules

G. BENZEKRI, O. MOUSSAOUI, A. ELMOUSSATI, A. BETARI
MATSI Laboratory (ESTO), Department of EIT (ENSAO)
Mohammed First University OUJDA, Mohammed V University Rabat
MOROCCO

Abstract: - In recent years, The Internet of Things (IoT) is considered as one of the main technological revolutions, it connects heterogeneous devices, peoples, and services in order to exchange information and to improve existing deployments in different sectors. So far, existing security solutions are not adapted to this development, considering that IoT resources are exposed to different intrusions, which impact security management efficiency and the need for human interventions to increase. Although, it is too hard to depend on manual approaches that require the deep involvement of security managers to deliver the aimed security level. Therefore, a new solution is needed, that will facilitate the decision against detected intrusions and according to their magnitudes and their intentions to put the necessary reaction in the right place. In this context, this paper proposes a model which specify how the decision and correlation scenario will be carried out when a critical alert comes from the intrusion detector basing on security policy rules. This model simplifies and facilitates the decision and reaction against detected intrusions by enriching it with the rules defined in security policy to ensure the protection of IoT resources and help security administrators to make the right decisions in other tasks.

Key-Words: - Internet of Things, security Intrusions, security management, decision, reaction, security policy rules.

Received: February 11, 2024. Revised: August 23, 2024. Accepted: September 26, 2024. Published: October 16, 2024.

1 Introduction

IoT stands for “Internet of Things” and refers to the growing trend of connecting physical devices to the internet and each other [1]. This includes everything from self-driving cars and smart homes to Wearables and industrial equipment. IoT devices are usually built with sensors and other components that allow them to collect data, which is then transmitted wirelessly to a central location where it can be processed and analyzed. The benefits of IoT include increased efficiency, improved safety and security, and even new business models.

With the proliferation of Internet of Things (IoT) devices in various domains, the security of these interconnected systems has become a critical concern [2]. IoT systems are vulnerable to a wide range of security threats and intrusions, which can have severe consequences on data integrity, user privacy, and system availability. Prompt detection and effective response to these intrusions are essential to mitigate potential damages and maintain the overall security posture of IoT environments.

In recent years, numerous approaches have been proposed for intrusion detection and response in IoT systems. However, many of these approaches focus primarily on the detection aspect, neglecting the crucial step of decision-making and response.

To address this gap, this paper proposes a model for the decision and response to detected intrusions in IoT systems, leveraging security policy rules as a guiding framework. Developing an effective decision reaction model is critical to the security of IoT devices and systems. By using a combination of techniques, it is possible to react to attacks quickly and effectively, limiting the damage they can cause and human intervention increase.

The proposed model will simplify the decision and reaction scenario against detected intrusion and it encompasses several key components. Firstly, the type and severity of detected intrusions is assessed based on predefined criteria and metrics. This severity assessment serves as a basis for determining the appropriate response actions to be taken. By incorporating security policy rules, the decision-making process is guided by a set of predefined rules that align with the organization's security objectives and policies.

The response actions can include isolating compromised devices, blocking suspicious network traffic, notifying stakeholders, initiating incident response procedures, and generating alerts for administrators or security teams. The proposed model contributes to the advancement of IoT security by providing a comprehensive framework that integrates the decision-making and response aspects

of intrusion management. By leveraging security policy rules, organizations can ensure consistent and effective responses to intrusions while aligning with their security objectives. Moreover, the model promotes proactive and context-aware decision-making, enabling timely responses to emerging threats and vulnerabilities.

Overall, this research aims to enhance the resilience and security of IoT systems by introducing a modeling framework that integrates security policy rules into the decision and response process for detected intrusions. By providing a structured approach to decision-making and response, organizations can effectively address the evolving security challenges in IoT environments and protect the integrity of their systems and data.

In the subsequent sections of this paper, we will provide a brief overview of Security management, Intrusion detection and security policy. After that we will present a state-of the art around related works. we will delve into the details of the proposed model, including the functionnement of the model, the formulation and implementation of security policy rules, the decision-making process, the response actions. Finally, we conclude by some perspectives.

2 Background and related work

This section gives an overview of the basic concepts necessary to understand the proposed framework whether in terms of architecture or functioning.

2.1 Security Management

Security management is a process that helps organizations safeguard their assets and protect against threats [3]. It includes identifying potential risks, assessing the impact of those risks, and implementing controls to mitigate or prevent them.

The burgeoning landscape of the Internet of Things systems introduces a paradigm shift in the way security is conceptualized and executed. Security Management in IoT systems is a multifaceted discipline designed to navigate the intricate challenges posed by the interconnectivity of devices and the diverse data streams they generate.

2.1.1 Risk Assessment and Mitigation

In the realm of IoT Security Management, proactive risk assessment takes center stage [4]. This involves a meticulous evaluation of potential threats and vulnerabilities unique to IoT ecosystems, providing a foundational understanding for subsequent security measures.

2.1.2 Holistic Data Protection

Beyond conventional data protection strategies, IoT Security Management addresses the intricacies of securing data throughout its life cycle, including storage, transmission, and processing on IoT devices [5]. This comprehensive approach reflects the recognition that safeguarding IoT data necessitates a multifaceted strategy.

2.1.3 Dynamic Anomaly Detection

An essential facet of Security Management in IoT is the incorporation of dynamic anomaly detection mechanisms [6] Leveraging cutting-edge machine learning algorithms allows for real-time analysis, enabling the identification of abnormal patterns or behaviors indicative of potential security breaches.

2.1.4 Fine-Grained Access Controls

Security Management strategies for IoT systems emphasize the implementation of fine-grained access controls [7]. This approach tailors access policies to restrict unauthorized interactions with IoT devices, mitigating the risk of unauthorized access and exploitation.

2.1.5 Standardized Frameworks for Resilience

Recent research underscores the critical importance of standardized security frameworks in enhancing resilience in IoT Security Management [8]. Collaborative endeavors aimed at establishing industry-wide standards make substantial contributions to the flexibility and strength of security protocols across the diverse IoT landscape.

Security Management in IoT systems represents a dynamic discipline that requires a nuanced comprehension of risks, the implementation of comprehensive data protection measures, adaptive anomaly detection, fine-grained access controls, and a bedrock of standardized frameworks. These components work in concert to bolster organizations against the ever-evolving threat landscape within the intricate ecosystem of the Internet of Things.

2.2 Intrusions Detections

An intrusion detection system (IDS) is a type of security software that monitors a network or systems for malicious activity or policy violations [9]. Any suspicious activity or violation is typically logged and an alert is generated to notify the administrator.
IDS comes in a variety of forms, including network-based IDS (NIDS), host-based IDS (HIDS), and application-based IDS (AIDS). Network-based IDS operates by analyzing incoming traffic and comparing it against a set of rules or signatures to

identify suspicious or malicious activity. Host-based IDS monitors activity on a single host, while application-based IDS specifically monitors activity within a certain application. There are many different types of IDS, but they all share the common goal of protecting against threats by detecting and logging suspicious activity.

2.3 Security policy

The Common Criteria defines an organizational security policy as: a set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment [10].
Security policy in IoT systems refers to a set of guidelines, rules, and procedures that define the measures and practices necessary to ensure the security and protection of IoT devices, networks, and data.

It encompasses various aspects, including access control, authentication mechanisms, encryption protocols, incident response procedures, and risk management strategies. The security policy acts as a roadmap for implementing and enforcing security measures throughout the lifecycle of IoT systems, from design and deployment to operation and maintenance. It establishes the framework for addressing potential vulnerabilities, mitigating risks, and complying with relevant regulations and industry best practices.

2.4 Security requirements:

In the ever-expanding realm of the Internet of Things (IoT), the establishment of robust security requirements is fundamental to mitigate the growing spectrum of threats. Security requirements in IoT systems encompass a comprehensive set of specifications that are pivotal for safeguarding data integrity, user privacy, and ensuring the resilience of interconnected devices [11], [12].

2.4.1 Data Encryption and Confidentiality

One primary security requirement in IoT systems involves the implementation of robust data encryption mechanisms [13]. Encryption is crucial for maintaining the confidentiality of data transmitted between IoT devices and ensuring that sensitive information remains secure from unauthorized access.

2.4.2 Authentication and Access Control

Authentication mechanisms play a vital role in validating the identity of IoT devices and users within the ecosystem [14]. Coupled with access control policies, these security requirements ensure that only authorized entities can interact with sensitive data and functionalities, mitigating the risk of unauthorized access.

2.4.3 Device Lifecycle Management

Effective management of the entire lifecycle of IoT devices is a critical security requirement. This involves secure onboarding, continuous monitoring, and secure decommissioning of devices to prevent vulnerabilities associated with outdated or compromised devices.

2.4.4 Integrity Verification

Security requirements mandate the implementation of integrity verification mechanisms to ensure the authenticity and unaltered state of transmitted data. Techniques such as digital signatures and hash functions play a crucial role in validating the integrity of information exchanged between IoT devices.

2.4.5 Secure Software and Firmware Updates

Regular updates to software and firmware are essential to address emerging vulnerabilities. Security requirements necessitate a secure update process that prevents tampering and ensures the authenticity of the updates, thereby maintaining the overall security posture of IoT systems.

2.4.6 Privacy-Preserving Mechanisms

Acknowledging the sensitivity of user data, privacy-preserving mechanisms constitute a significant security requirement. Techniques such as anonymization and differential privacy are crucial for safeguarding user privacy in IoT ecosystems.

2.4.7 Resilience against Denial-of-Service Attacks

Security requirements in IoT systems include provisions for resilience against denial-of-service attacks. Robust network architecture and traffic monitoring mechanisms are imperative to detect and mitigate the impact of such attacks, ensuring uninterrupted service availability.

adherence to stringent security requirements is paramount for fostering trust and resilience in IoT systems. By integrating encryption, authentication, lifecycle management, integrity verification, secure updates, privacy preservation, and resilience against attacks, organizations can establish a robust security framework in the IoT landscape.

2.5 Related Works

The rapid proliferation of interconnected devices with diverse characteristics poses a significant challenge for network administrators tasked with managing these devices. Security has emerged as a

critical concern in today's Internet landscape, given the increasing sophistication of security attacks.

Moreover, addressing security threats in the IoT realm is particularly challenging due to the limited storage capacity, energy constraints, and processing capabilities of these devices. These limitations render existing network security mechanisms, such as firewalls and IDS/IPS, inadequate for effectively mitigating security risks in IoT environments.

Consequently, researchers in this field have shifted their focus towards developing new approaches to address both security management and security challenges cited in section 2 aimed at organizing and managing IoT systems more efficiently.

The proposition in [15] centers on access control within the IoT framework by introducing a dynamic and fully distributed security policy. its will leverage the block chain concept to ensure robust distributed capabilities, which are highly recommended in IoT environments. Additionally, it's based on machine learning algorithms, specifically focusing on reinforcement learning techniques, to deliver a dynamic, optimized, and self-adjusting security policy.

In [16] authors have introduced and explored a versatile framework for enforcing security and data quality, seamlessly integrated into a distributed IoT middleware platform. The framework presented facilitates the implementation of security and data quality enforcement policies that can be applied across various domains and are capable of identifying violation attempts.

In fact, in [17] authors proposed a dynamic security management model with the goal of streamlining the security management process. However, there are still areas of improvement that we plan to address in future research. Specifically, we aim to develop a dynamic policy framework that considers the contextual factors surrounding smart devices. Additionally, this framework will be capable of evolving over time, leveraging the vast and varied data generated by IoT devices.

The authors in [18] present a Model-Driven Security policy enforcement framework called MDSIoT, designed for IoT tenant applications deployed on edge servers. This framework enables the specification of execution policies at the model level, which are then translated into code for deployment and enforcement at runtime.

This paper [19] revolves around the utilization of a sequential model, which serves as a foundational aspect for introducing novel methodologies. These methodologies are tailored to leverage the unique capabilities of the model. Specifically, the model is capable of gathering features from both the network layer, through tcp dump packets, and the application layer, via system routines. Based on this finding, a sequential model-based intrusion detection system, employing deep learning techniques, holds promise for enhancing the security of IoT servers.

3 Discussion and proposed model

3.1 Discussion

After an exhaustive review of existing literature on IoT security challenges and security management, it is apparent that most of these works focus primarily on policy enforcement for security, access control, and intrusion detection. However, it is clear that many proposed approaches in security management primarily emphasize detection, often overlooking critical decision-making and response phases.

Indeed, current solutions do not adequately address all the identified IoT security challenges outlined in the background. Therefore, there is a need for a new solution that can effectively manage security in a manner more suited to the evolving nature of existing and future networks, characterized by their openness, complexity, and dynamism, and that can address all IoT security challenges comprehensively.

Relying solely on manual approaches that require extensive involvement from security managers to achieve the desired security level is challenging. Hence, any security management approach should be comprehensive, aiming to establish a security platform that supports solutions and products working independently towards a common objective.

Consequently, there is a pressing need for a model that specifically addresses the intricacies of decision and response to detected intrusions in IoT systems, emphasizing the utilization of security policy rules as a guiding framework.

The development of an effective decision reaction model is paramount for ensuring the robust security of IoT devices and systems. Through the integration of various techniques, it becomes imperative to establish a system that enables swift and efficient reactions to attacks, thereby mitigating potential damage and reducing the reliance on manual human intervention.

To streamline the decision and reaction scenario against detected intrusions, the model encompasses several key components. Primarily, it evaluates the type and severity of detected intrusions based on predefined criteria and metrics. This severity

assessment forms the foundation for determining the most appropriate response actions. The incorporation of security policy rules into the decision-making process ensures that responses are guided by a set of predefined rules aligned with the IoT systems overarching security objectives and policies.

Potential response actions include isolating compromised devices, blocking suspicious network traffic, notifying stakeholders, initiating incident response procedures, and generating alerts for administrators or security teams. The overarching goal of the model is to contribute significantly to the progression of IoT security by providing a comprehensive framework that seamlessly integrates decision-making and response aspects within the realm of intrusion management. Leveraging security policy rules ensures a consistent and effective response to intrusions, harmonizing with the IoT systems security objectives. Furthermore, the model fosters proactive and context-aware decision-making, facilitating timely responses to emerging threats and vulnerabilities.

3.2 Proposed Model

In this section, we will present the decision reaction model and we will discuss the role of its components. So, development of this model will be like a database model and based mainly on three questions about critical alert to simplify the comprehension of model working:

a) Should we react or not?
b) At what level to react?
c) How should we react?

The "Fig. 1" presents the global view of this model.

Fig. 1: Proposed model

So, we were able to specify the different knowledge that can be modeled, which will be used in the process of attack analysis, correlation, decision making, and reaction.

a) Should we react or not?

The management and decision-making process is the core of the model. Indeed, he receives a critical alert that an attack targets an asset in the IoT system. Either the attack is successful, it was considered an intrusion or it remains an unsuccessful attack.

The management and decision-making process will make the decision to react or not to an attack according to two criteria: the severity of the attack and the criticality of the resources and the types of reaction which can be applied.

Regarding the severity of the attack, the management and decision-making process must be able to analyze the attack based on its information; Attack: @source, @destination, protocol, nature of the attack target, its criticality, path of the attack, the connection, the number of transactions, and the number of authentication failures. The attack information will be in a single table named Attack like the "Fig. 2".

Fig. 2: Attack table

However, an attack can target a specific configuration file, backup file, or service. Typically, the targeted goods can be anything that is produced (concrete) at the level of the IoT system. However, in our case, we will just focus on the resources that present intelligent IoT devices (sensors, actuators, gadgets, appliances, machines…).

In addition, the classification of resources according to their degree of criticality and the types of reactions that can be applied is an important point. Indeed, the degree of criticality of a resource is classified according to its impact on the performance of the IoT System. Already at the reaction level, we must take into account the main objectives of security: availability in the first place (case of denial of service), confidentiality, and integrity (non-repudiation and authentication).

Thus, the types of reactions that can be applied differently from one resource to another, which translate into rules to be applied. In the event that the attack does not represent seriousness and the resource is not classified as critical and there will be no reaction, the event must be recorded in an event log in order to be analyzed by the following. At this level,

we must model the resources that present all's resources of the IoT system as well as the various reactions which can be applied since each resource has its own specifications (possible reactions on each resource).
In this case, we have inspired by the DEN-ng model [20] which models a resource with its specifications as shown in "Fig. 3".

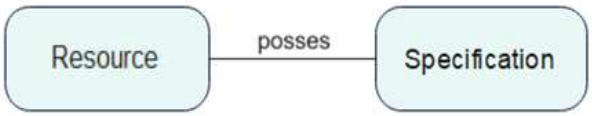

Fig. 3: Resource and Specification tables

b) At what level to react?

In case that the decision will be to react, we must specify where the reaction will be applied, so it is necessary to know how the resources are interconnected in the IoT network. In this case we will refer to the network topology which describes how the network entities are directly linked to each other and define the way in which information can flow. Thus, the network topology gives us a vision of the location of the resources of the information IoT system and describes the architecture of the network by representing all interfaces and the links between them. The representation of the network topology intervenes in the decision-making process to react against an attack. Thus, we can locate a machine in the network by searching on which interface are connected and linked. At this level, we must model how resources are interconnected between them in order to react correctly to attacks.
In the context of our work, we will use two tables "Fig. 4", a resource table which will bring together the various resources, and an interfaces table which includes the information @ IP of the interface, the subnet mask, and the default gateway. Since each resource is linked to another by an interface and each interface is characterized by @ IP, a subnet mask, and a gateway.

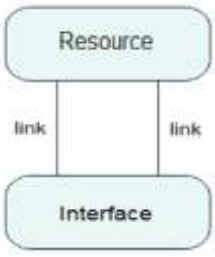

Fig. 4: Resource and Interface tables

At this level we need to model the event that controls the verification that the management and decision-making process performs between the attack that exceeds a rule applied to a given resource and the adequate reaction. In this context, we referred to the management policy PBNM from DEN-ng model [21] which is used as a means of controlling the behavior of a managed system. This notion has been used in research work concerning autonomous networks in order to manage control loops. However, the management policy is defined as a set of rules. Each policy rule consists of a condition clause and an action clause. Policy is generally represented as a set of classes and relationships that define the semantics of policy representative building blocks. These building blocks usually consist of a minimum of a policy rule, a policy condition, and an action policy and an event handler and are represented as illustrated in "Fig. 5".

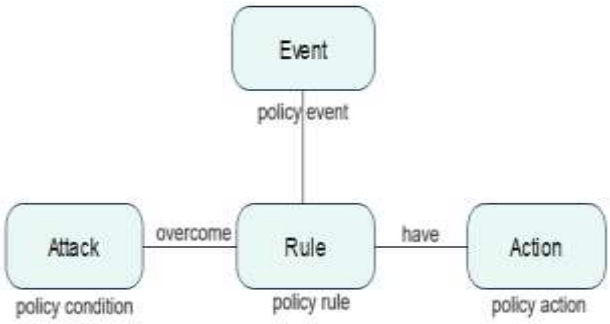

Fig. 5: building blocks policy

As part of our work, the decision-making management subsystem checks between the attack and the rules applied to the resources, based on this verification and this analysis, it gives a decision in the form of " a set of actions to apply. Thus, the template reads as follows:

•An attack exceeds a rule applied to an IOS resource.

•An event is triggered which checks between the attack and the outdated rule to establish a set of actions to apply.

•The set of actions will be applied to the resources that are linked together via interfaces (modeling the network topology), the way they are connected will facilitate the task of specifying the location of the reaction (at what level to react).

c) How should we react?

The proposed model enhances the ability to promptly detect intrusions, assess their severity, and initiate appropriate response actions based on predefined security policy rules. By integrating security policy rules into the decision and response process, organizations can ensure a structured and consistent approach to mitigating security risks in IoT environments.

The description of the decision-making and reaction process will be facilitated by explaining it in the form of a scenario as follows:

1)First of all, every information system has a security policy that has been established as part of the development of a security framework. Indeed, the security policy will define the various security rules applied to the resources. An attack originating from inside or outside the system, if it targets a given asset, it will exceed the security rules applied to the resources.

2)After the rule is exceeded, the subsystem will check the attack information (path of the attack, destination, all the resources it has exceeded and make the comparison with the rules of the security policy applied on the resources.

3)After the verification and comparison is carried out, the reaction can be either the modification of an already existing rule, or the creation of a new rule (Taking into account the importance of the availability of the System (case of denial of service), the system must be preventive).

At this level, learning techniques must be involved in order to have an extensible knowledge base that is regularly fed with each attack event = reaction, the techniques of 'learning will be likened to a diagnosis (case of doctors' diagnoses).A diagnosis that will classify reactions until the best solution is found and kept (which of course remains extensible),for example , an attack exceeded a rule applied on a resource, the system according to its analysis chose to modify it, subsequently, another attack attempt exceeded the same rule applied, so the modification did not lead to a result on, therefore it is necessary to improve the modification of the rules until finding the right rule (which remains extensible) and which will be used subsequently to react automatically to such an attack.

4 Conclusions and future work

In conclusion, this article has presented a novel approach for modeling the decision and response to detected intrusions in IoT systems, leveraging security policy rules as a guiding framework.

The suggested model improves the capacity to quickly identify intrusions, evaluate their seriousness, and activate suitable response measures according to pre-established security policy guidelines. By incorporating security policy guidelines into the decision-making and response framework, organizations can guarantee a methodical and uniform method for mitigating security threats in IoT settings.

The application of the proposed model offers several benefits. It enables proactive decision-making, allowing organizations to respond swiftly to emerging threats and vulnerabilities. The use of security policy rules ensures that response actions align with organizational security objectives and compliance requirements. Additionally, the model promotes context-aware decision-making, taking into account the specific characteristics and constraints of the IoT environment.

Future research endeavors could focus on several areas to further enhance the modeling approach. Firstly, exploring advanced machine learning and artificial intelligence techniques for intrusion detection and severity assessment could improve the accuracy and effectiveness of the model. Additionally, incorporating dynamic and adaptive security policy rules that can evolve with changing threat landscapes would enhance the model's resilience and responsiveness.

Furthermore, investigating the scalability and resource utilization of the model in large-scale IoT deployments would provide valuable insights for practical implementation. The evaluation of the model in diverse IoT domains and real-world scenarios would help validate its effectiveness and identify any domain-specific considerations or challenges.

Overall, the modeling approach presented in this article lays the foundation for enhancing the decision-making and response capabilities in IoT systems. By leveraging security policy rules, organizations can effectively mitigate intrusions, safeguard sensitive data, and maintain the security and trustworthiness of their IoT environments. Future research efforts in this direction will contribute to advancing the field of IoT security and addressing the evolving challenges posed by emerging threats and technologies.

Acknowledgement:

This work is supported by the Mohammed First University under the PARA1 Program

References:

[1] A. H. Hussein, “Internet of Things (IOT): Research Challenges and Future Applications,” 2019. [Online]. Available: www.ijacsa.thesai.org

[2] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W. C. Hong, “Internet of things: Evolution, concerns and

security challenges," Sensors, vol. 21, no. 5, pp. 1–35, Mar. 2021, doi: 10.3390/s21051809.

[3] M. Zammani, R. Razali, and D. Singh, "Organisational Information Security Management Maturity Model." [Online]. Available: www.ijacsa.thesai.org

[4] J. R. C. Nurse, S. Creese, and D. De Roure, "TRUSTING THE INTERNET OF THINGS Security Risk Assessment in Internet of Things Systems," 2017.

[5] C. Chong, K. Lee, and G. Ahmed, "Improving Internet Privacy, Data Protection and Security Concerns." [Online]. Available: https://journals.gaftim.com/index.php/ijtim/issue/view/1PublishedbyGAF-TIM,gaftim.com

[6] A. Sarwar, A. M. Alnajim, S. N. K. Marwat, S. Ahmed, S. Alyahya, and W. U. Khan, "Enhanced Anomaly Detection System for IoT Based on Improved Dynamic SBPSO," Sensors, vol. 22, no. 13, Jul. 2022, doi: 10.3390/s22134926.

[7] Q. Zhou, M. Elbadry, F. Ye, and Y. Yang, "Towards Fine-Grained Access Control in Enterprise-Scale Internet-of-Things," IEEE Trans Mob Comput, vol. 20, no. 8, pp. 2701–2714, Aug. 2021, doi: 10.1109/TMC.2020.2984700.

[8] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities," IEEE Communications Surveys and Tutorials, vol. 22, no. 4, pp. 2489–2520, Oct. 2020, doi: 10.1109/COMST.2020.3011208.

[9] R. H. Mohamed, F. A. Mosa, and R. A. Sadek, "Efficient Intrusion Detection System for IoT Environment," International Journal of Advanced Computer Science and Applications, vol. 13, no. 4, pp. 572–578, 2022, doi: 10.14569/IJACSA.2022.0130467.

[10] A. Ghazvini, Z. Shukur, and Z. Hood, "Review of Information Security Policy based on Content Coverage and Online Presentation in Higher Education," 2018. [Online]. Available: www.ijacsa.thesai.org

[11] S. Pal, M. Hitchens, T. Rabehaja, and S. Mukhopadhyay, "Security requirements for the internet of things: A systematic approach," Sensors (Switzerland), vol. 20, no. 20, pp. 1–34, Oct. 2020, doi: 10.3390/s20205897.

[12] M. Imdad, D. W. Jacob, H. Mahdin, Z. Baharum, S. M. Shaharudin, and M. S. Azmi, "Internet of things (IoT); security requirements, attacks and counter measures," Indonesian Journal of Electrical Engineering and Computer Science, vol. 18, no. 3, pp. 1520–1530, 2020, doi: 10.11591/ijeecs.v18.i3.pp1520-1530.

[13] A. Yousefi and S. Mahdi Jameii, "Improving the Security of Internet of Things using Encryption Algorithms."

[14] J. I. Zong Chen and K.-L. Lai, "Internet of Things (IoT) Authentication and Access Control by Hybrid Deep Learning Method - A Study," Journal of Soft Computing Paradigm, vol. 2, no. 4, pp. 236–245, Jan. 2021, doi: 10.36548/jscp.2020.4.005.

[15] A. Outchakoucht and J. P. Leroy, "Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things," 2017. [Online]. Available: www.ijacsa.thesai.org

[16] S. Sicari, A. Rizzardi, D. Miorandi, C. Cappiello, and A. Coen-Porisini, "Security policy enforcement for networked smart objects," Computer Networks, vol. 108, pp. 133–147, Oct. 2016, doi: 10.1016/j.comnet.2016.08.014.

[17] G. Benzekri, O. Moussaoui and A. El Moussati," IoT Security Management: Model and Design Issues", LNEE, Advances in Smart Technologies Applications and Case Studies, pp. 212–219, Aug. 2020

[18] P. H. Nguyen, P. H. Phung, and H. L. Truong, "A security policy enforcement framework for controlling IoT tenant applications in the edge," in ACM International Conference Proceeding Series, Association for Computing Machinery, Oct. 2018. doi: 10.1145/3277593.3277602.

[19] M. Zhong, Y. Zhou, and G. Chen, "Sequential model based intrusion detection system for iot servers using deep learning methods," Sensors (Switzerland), vol. 21, no. 4, pp. 1–21, Feb. 2021, doi: 10.3390/s21041113.

[20] D. Kontoudis et P. Fouliras, " A Survey of Models for Computer Networks Management ", International journal of Computer Networks & Communications, vol. 6, no 3, p. 157 176, mai 2014, doi: 10.5121/ijcnc.2014.6313.

[21] Korean Information and Communications Society. Technical Committee on Korean Network Operations and Management, Denshi Jōhō Tsūhin Gakkai (Japan). Technical Committee on Information and Communication Management, IEEE Communications Society, et Institute of Electrical and Electronics Engineers, APNOMS 2017 : the 19th Asia-Pacific Network Operations and Management Symposium : " Managing a World of Things " : Sep. 27-29, 2017 in Seoul, Korea.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.