Manufacturing Science and Education 2025

ACTA TECHNICA NAPOCENSIS

Series: Applied Mathematics, Mechanics, and Engineering
Vol. 68, Issue Special II, July, 2025

RESEARCH REGARDING THE SAFE USE OF INTERCONNECTED SMART DEVICES ON THE INTERNET OF THINGS

Valentin MANIU, Cosmin PIELE

Abstract: *The Internet of Things (IoT) constitutes a globally interconnected network of computing, sensing, and networking devices that facilitate data exchange through diverse communication protocols. Recent advancements in technologies have significantly enhanced the seamless integration of smart devices. Consequently, the selection of an optimal network security design is imperative for system architects, necessitating a thorough evaluation of networks not only in terms of connectivity but also from a security standpoint. This article depicts a detailed analysis of IoT architecture, device security, and associated challenges in maintaining security requirements for IoT devices. It explores various cyber threats, their attack mechanisms, and potential mitigation strategies. Furthermore, the study outlines future directions to adopt the security challenges of next-generation IoT systems. The empirical data of this study is to offer a clear summary of IoT security, cyberattacks, and prospective solutions, offering valuable insights for both academics and industry professionals across diverse contexts.*
Keywords: *architecture of IoT, device security, cyber threats, mitigation strategies.*

1. INTRODUCTION

The Internet of Things (IoT) is rapidly evolving, integrating into nearly every aspect of our lives while raising concerns about the security of these interconnected devices. Its exponential growth has created an expansive attack surface with potentially severe consequences. As IoT devices handle vast amounts of sensitive data and control critical systems, they have become prime targets for cyberattacks, data breaches, and malicious exploits. Weak encryption, inadequate security measures, and irregular update policies leave many IoT systems dangerously exposed. The complexity and diversity of these ecosystems further complicate the task of securing them against sophisticated, ever-evolving threats.

This study aims to into the core aspects of IoT security by analyzing its fundamental architecture, essential protective measures and common threat avenues. We strive to identify vulnerabilities and uncover new research directions through a comprehensive analysis.

Ensuring security is paramount in minimizing the attack surface and preventing vulnerabilities, especially as IoT technology is increasingly deployed in critical sectors such “as the economy and national security, each with distinct industry standards and requirements. Beyond cyberattacks, the development of large-scale, heterogeneous networks composed of resource-constrained nodes operating in real time must be supported by an architecture that accounts for factors such as reliability, quality of service, modularity, semantic interoperability, privacy management, and seamless hardware-software compatibility” [1].

2 FRAMEWORK

2.1. Motivation

The IoT is rapidly evolving, integrating into every aspect of our lives, yet raising concerns about the security of these interconnected devices. Its widespread adoption in multidomain environments has significantly expanded the attack surface, posing potential risks with far-reaching consequences. This study is guided by the need to explore IoT security, focusing on its

underlying architecture, essential security aspects, and exploring surface of cyber-attack.

2.2. Methodology

To comprehend the complexity and dynamism of security assurance in IoT systems, a structured review of the existing literature was undertaken to answer the following research questions.:

RQ1: How do different IoT architectural models impact the security and efficiency of IoT networks, and what are the key trade-offs between security and performance across the architectural layers?

RQ2: What kind of attacks are a threat of IoT systems, and what is the best mitigation?

To ensure the accuracy of the results, a selection of specialized literature was conducted based on specific keywords, incorporating terms such as "IoT Architecture," "IoT Communication Protocols," "IoT Security Issues and Concerns," and "IoT Applications." These keywords were used to search various scientific repositories, in this particular case we use from our interrogation the database "Web of Science" to identify an initial set of relevant research sources. The interrogation was whit logical parameter "or". After the initial query, a total of 3460 reviewed articles resulted.

Then making this selection, we proceeded to restrict the data set, by applying conditions such as reputation, importance of the source, date of publication, impact factor and open access.

The work is structured as follows: Firstly, it presents a comprehensive overview of present study on the classification and security tasks of IoT devices. Secondly it delves into the generic architecture of IoT systems. The subsequent section focuses on the fundamental security requirements that IoT devices must fulfill. This is followed by an analysis of various cyber threats, their impact on IoT systems, and corresponding mitigation strategies at each architectural layer. Furthermore, the paper examines recent IoT security incidents and their implications. Finally, the concluding section summarizes the key findings and outlines potential directions for future research.

3 CLASSIFICATION AND SECURITY CHALLENGES OF IOT

The classification of attacks based on OSI model layers is discussed by both [2] and [3]. The diversity of security attacks on RFID systems is addressed in [4], while [5] presents both various attacks on these systems and possible solutions. A general categorization of attacks is proposed in [6], where they are classified into four main categories based on their properties and target layer: encryption attacks, software attacks, network attacks, and physical attacks.

Sicari et al. identify research challenges and potential methodologies for enhancing IoT security, "*categorizing them into eight key areas: (1) appropriate authentication mechanisms, (2) privacy, (3 access management rules, (4) trust issues, (5) implementation of security rules, (6) mobile security, (7) intermediary security, and (8) privacy policies*" [7].

In real-world scenarios, millions of devices communicate with each other, some handling sensitive data from users' personal spaces, transmitted over the Internet. This significantly increases the risk of data privacy breaches. In [8], "*various privacy policies have been proposed, tailored to different data types, targeting to protect user privacy*". Each confidentiality zone corresponds to a distinct contextual environment and attested through a Core-Center before approving connection or re-registration requests to prevent unauthorized data sharing. However, risks related to smart devices that bypass Core-Center connectivity were not addressed.

Dey et al. "*explore big data applications generated by IoT and how to manage data from sensors and embedded devices*". Their contribution covers applications such as smart cities, industrial IoT, healthcare, autonomous sensor networks, smart and sustainable green cities [9]. They also provide a detailed explanation of electronic health record security, testing the system against potential attacks. Security challenges for IoT-generated big data, including side-channel attacks, are also discussed.

Hassanien et al. examine challenges "*related to the Internet of Medical Things (IoMT),*

proposing solutions for managing big medical data" along with recent classification and machine learning techniques [10]. They also address data privacy concerns and security analysis within the IoMT context. With the rapid growth of digital communication and data digitization in recent years, this trend is expected to continue as IoT advances.

Sarowar et al. provide examples "*of messaging mechanisms in M2M communication, mobile computing, and sensor networks. They introduce novel techniques for detecting location spoofing, efficient processing strategies, and clustering tools for next-generation applications*" [9].

4. ARCHITECTURE MODEL OF THE IOT

"*Architecture is the structured framework that delineates the physical elements of a network and its functional arrangement and setup, encompassing its operational principles, procedures, and data formats employed in its functioning*" [11]. The "*IoT architecture encompasses an assemblage of physical entities, sensors, cloud services, developers, actuators, communication layers, users, business layers, and IoT protocols* [12]. *Owing to the extensive scope of the IoT, there is no universally accepted consensus on a single IoT architecture. Various researchers have proposed different architectural models to address the diverse facets of the IoT*" [13]. According to most scientists, "*IoT architecture is commonly conceptualized as consisting of primary layers: perception, network, middleware, and application layers*" [14, 15].

4.1. Key Layers of IoT Architecture

Understanding the fundamental layers of IoT architecture is essential for grasping its capabilities and ensuring effective implementation. The primary layers include the perception/sensing layer, connectivity/network layer, data processing layer, and user interface/application layer. Each of these components plays a crucial role in integrating an efficient IoT system. The proposed IoT architecture is depicted in Figure 1.

4.1.1. Physical Layer

The Physical Layer comprises physical link that serves as the foundation of IoT technology. Their primary function is to gather information, convert it into digital data, and transmit it to the next layer for further processing and action. According to Hassan "*this layer is acting as a bridge between the digital and physical worlds, these devices include sensors (e.g., temperature, humidity, light), actuators (electric, mechanical, hydraulic), RFID systems (RFID tags), video trackers (IP cameras), and any other components capable of utilizing data to interact with various devices over a network*" [16].

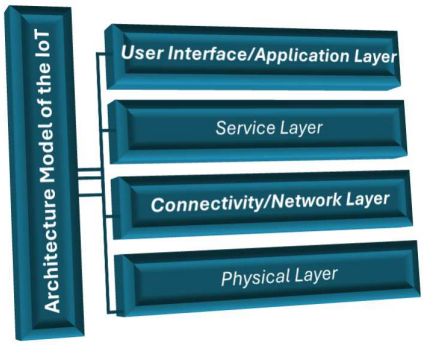

Fig.1. IoT Architecture Source: Own contribution

4.1.2. Connectivity/Network Layer

Connectivity or Network Layer enables the transmission of digital data between different IoT components. It utilizes communication protocols such as HTTP, MQTT, and AMQP to ensure smooth data exchange. To maintain data integrity, security measures like asymmetric key encryption are implemented with public and private key cryptography ensuring that only authorized recipients can decrypt the transmitted information. Additionally, private 5G networks enhance security by providing full control over data flow. Essential elements of this layer include internet gateways, intranet ports, network gateways, and Data Acquisition Systems (DAS), all working together to facilitate efficient device interconnectivity Data Processing Layer [16].

4.1.3. Service Layer

The main goal of this service layer is to bring together various operations, forming an affordable platform. It manages service coordination, communication, data exchange, and storage while facilitating service discovery to identify entities that provide necessary services and information.

A key example of this concept is cloud computing, which provides "*hardware, software platforms, protocols, and applications, along with storage and data analysis capabilities for IoT. However, due to the complexity and diversity of IoT architecture, this layer faces significant security challenges. These challenges are even more prominent in cloud environments, involving concerns such as user authentication, data security, and privacy protection. Ensuring cloud service availability is critical, as users seek transparency regarding data management and storage locations*" [17]. In this case, cloud service contributors must implement robust security policies and assurances to safeguard user data and prevent its unauthorized use.

4.1.4. User Interface/Application Layer

The Application Layer sits above the Service Layer and can be structured in various ways depending on its implementation. Its primary function is to analyze and process data received from the lower layers. Specifically, it manages this data by delivering it to applications for execution, such as controlling actuators, forwarding it to other points, "*or passing it to another application for further processing. Additionally, this layer often includes the user interface (if applicable), allowing users to interact with the IoT system and perform necessary actions. For instance, if a piece of technical equipment requires maintenance, the IoT system can notify the technician through an interface that operates within the Application Layer*" [18].

5. ESSENTIAL SECURITY FEATURES OF IOT

IoT faces ongoing threats to security resulting from the diversity of its devices and limited computing and power resources of IoT devices, leading to additional concerns. To establish a secure IoT system, it is essential to integrate the security features throughout both the development and operational phases of IoT devices. The most important security features will be outlined in the following section. The CIA triad is a cornerstone model in cybersecurity, encompassing three essential principles: confidentiality, integrity, and availability. A schematic representation of this model is provided in Figure 2.

Fig.2. CIA TRIAD
Source: Office of Energy Efficiency & Renewable Energy

5.1. Confidentiality

Confidentiality ensures "*that information is accessible only to authorized entities. Protecting data involves restricting access, allowing only authorized users, and preventing devices from sharing data with neighboring entities, including services, individuals, or other devices*" [19]. Various security mechanisms, including mechanisms such as two-factor authentication and cryptographic data protection, are available to maintain data confidentiality. However, these methods often require significant computational resources. Therefore, sensors must implement encryption mechanisms that align with their computational and energy constraints. In addition, the definition of a secure IoT service that ensures reliable data access and management is crucial for safeguarding system integrity and confidentiality.

5.2. Integrity

In the IoT ecosystem, the importance of data integrity is often underestimated. Ensuring "*data integrity is crucial, as it involves verifying the authenticity of the sender and confirming that the data remains unaltered throughout transmission, despite potential interference from*

attackers, users, or eavesdroppers" [20]. However, these methods are insufficient for securing IoT endpoints.

5.3. Availability

"*Availability is a critical guarantee that a system will operate reliably under all conditions, making it a vital feature of IoT, particularly in essential sectors. For instance, in health monitoring systems, the real-time collection of patient data is crucial, as any disruption in availability could have life-threatening consequences*" [21]. Maintaining IoT system readiness, requires a seamless amalgamation of several factors, including energy-efficient protocols, energy harvesting techniques, and lightweight yet effective encryption mechanisms. However, the complexity and heterogeneity of IoT infrastructure further challenge availability, making it vulnerable to energy depletion attacks.

6. VARIOUS CYBER THREATS TARGETING IOT LAYERS

The growing concern over IoT security is driven by the increasing frequency of attacks on embedded devices. This section highlights the main types of attacks targeting the IoT framework.

6.1. Cyber Threats and Possible Physical Layer Attacks

Physical layer attacks are chiefly intended to impede communications and obstruct data collection operations [22]. The table below presents an overview of the identified attacks, detailing their impacts and outlining the corresponding mitigation strategies.

Table 1

Common Attacks on the physical layer: Impacts and Mitigation Strategies

Source: Own contribution

Attacks	***Impact***	***Mitigation***
Physical interception	Stolen or compromised sensitive data.	Implement physically secure communication techniques and enforce encryption measures.
Unauthorized physical access or device theft.	Unauthorized access may lead to the exposure of confidential information, device alterations, or resale on dark-web	Enhance physical security, implement locks, and secure containers. If unauthorized access is detected, implement a breach alert system.
Jamming	Loss of data or device failure.	Implementing anti-jamming strategies
Electromagnetic Interference (EMI)	Data integrity issues, system failures, or irreversible hardware damage	Perform electromagnetic compatibility (EMC) assessments and implement protective measures to shield IoT devices from electromagnetic interference (EMI)
e engineering	Attackers can exploit vulnerabilities compromising security and confidentiality.	Implementing hardware obfuscation techniques, manipulate packaging, and regular security audits.

6.2. Attacks on the Connectivity/Network Layer of the IoT architecture

Table 2

Common Attacks on the connectivity/network layer: Impacts and Mitigation Strategies Source: Own contribution

Attacks	***Impact***	***Mitigation***
Man-in-theMiddle (MitM)	Enabling attackers to intercept and manipulate crucial information.	Implement strong authentication methods and encryption protocols
Spoofing	Loss of network integrity, enabling unauthorized infiltration	Enhance network protection by using certificate authentication and intrusion detection systems to monitor abnormal behavior.
DoS&DDoS	Disrupt IoT services, making devices and networks inaccessible, leading to widespread operational failures.	Implement traffic filtering mechanisms, robust device authentication protocols, and rate limiting techniques to detect and prevent unauthorized or malicious communications within the network

The conectivity/network layer is essential to maintaining data protection and enabling network communication. Below, in table 2, are several common threats/attacks, along with a summary of their impacts and mitigation strategies.

6.3. Attacks on the Service Layer

By exploiting vulnerabilities in the services layer, Malicious users can disrupt the application layer, which provides essential services. These attacks primarily target data center infrastructure, including Bare Metal, Dedicated, and Cloud Servers. The subsequent section examines these attacks, their implications, and potential mitigation strategies,

as represented in Table 3.

Table 3

Common Attacks on the Middleware Layer: Impacts and Mitigation Strategies Source: Own contribution

Attacks	*Impact*	*Mitigation*
Flood attack	Compromise reliability and availability.	Implement rate limiting, traffic management, load balancing, and anomaly detection techniques to enhance security and optimize performance.
Browser-based cloud attack	Unauthorized individuals gaining access to sensitive data.	Implement secure browsing practices and is mandatory to use a Web Application Firewall (WAF).
Replay attack	Malicious actors can circumvent authentication mechanisms by replaying previously valid authentication tokens or credentials, thereby compromising system security, facilitating data infringements, and enabling unauthorized control over IoT devices.	Integrate timestamps and nonces (random, single-use numbers) into communications to ensure each message is unique and cannot be reused outside its valid time frame. Additionally, employ session tokens with restricted validity periods, refreshing them periodically to prevent the exploitation of expired or intercepted tokens. These measures enhance security by mitigating replay attacks and ensuring authentication integrity.
Privilege escalation	Aggressors can exploit vulnerabilities to access restricted data and mission-critical operation which may lead to data breaches and unauthorize control or alteration of Io devices.	Deploy strong admission control measures based on a risk matrix to authorize multi-level access

6.4. Attacks on the Application Layer

The application layer serves a pivotal function in provisioning dynamic, user-oriented services and functionalities., while also processing and interpreting data transmitted from the network layer "*This layer is primarily vulnerable to software-based attacks and permission-related security risks throughout a device's lifecycle. Such attacks often aim to access sensitive user information, potentially compromising data confidentiality and privacy*" [23]. The table 4 outlines specific attacks, their impact, and corresponding mitigation strategies.

Table 4

Common Attacks on the Application Layer: Impacts and Mitigation Strategies Source: Own contribution

Attacks	*Impact*	*Mitigation*
Phishing	Obtains confidential data, including usernames and passwords.	Implement multi-factor authentication schemes and promote user awareness.
Session hijacking	This vulnerability may allow adversaries to access sensitive data and gain unauthorized control over IoT devices.	To strengthen physical security, implement hardware-based protections such as locks, tamper-evident seals, and secure enclosures. Additionally, deploy intrusion detection systems (IDS) to monitor for unauthorized access attempts and generate real-time alerts.
Injection of code	*Compromise passwords, expose confidential data, gain unauthorized system access, extract sensitive information, or deploy self-replicating malware.*	*Implement authentication measures, conduct regular similarity analysis, and perform system testing prior to installation.*
Zero-day exploit	Lead to significant security vulnerabilities and unauthorized access to IoT data or devices.	Implement proactive security measures such as vulnerability management and continuous security monitoring
Authorization	This vulnerability occurs when an attacker exploits weaknesses or circumvents an application's authorization mechanisms, gaining unauthorized access to protected resources or performing actions exceeding their granted permissions	Implement stringent access policies to regulate and control permissions for different system resources

7. CONTRIBUTION

Following the elaboration of the work, the resulting scientific contributions are as follows:

- ***Comprehensive Classification of IoT Security Threats***:

The paper systematically categorizes IoT security threats based on the OSI model layers, highlighting specific attack vectors at each layer. It identifies key threats such as physical attacks (e.g., jamming, reverse engineering), network-based attacks (e.g., MitM, DoS/DDoS), service-layer attacks (e.g., replay attacks, privilege escalation), and application-layer attacks (e.g., phishing, session hijacking). By mapping these threats to corresponding mitigation strategies,

the paper provides a structured approach to understanding IoT security challenges.

- ***Classification of Security Measures Across IoT Architecture***:

The study outlines the essential security features required for IoT systems – confidentiality, integrity, and availability – while emphasizing the difficulties arising from the limited resources of IoT devices. By addressing security at multiple architectural layers, the paper highlights a holistic approach to enhancing IoT resilience against cyber threats.

8. CONCLUSION

The rapid proliferation of IoT technologies has revolutionized multiple industries, offered numerous benefits while simultaneously introduced significant security challenges. This study has provided a comprehensive analysis of IoT security by examining its architecture, identifying critical security features, and categorizing various cyber threats targeting IoT layers. The findings highlight the vulnerabilities inherent in IoT ecosystems, primarily due to the diverse and resource-constrained nature of devices, the heterogeneity of communication protocols, and the growing sophistication of cyberattacks. The study underscores the importance of ensuring confidentiality, integrity, and availability to safeguard IoT systems. Effective security mechanisms, such as encryption, authentication protocols, and anomaly detection systems, play a crucial role in mitigating risks. However, given the increasing volume of cyber threats, traditional security measures alone are insufficient. AI-driven security solutions, adaptive intrusion detection systems, and blockchain-based authentication methods represent promising advancements in IoT security.

In conclusion, IoT security remains a pressing concern, necessitating continuous efforts to develop robust and scalable solutions. While advancements have been made, the ever-evolving threat landscape requires further research and innovation to enhance security mechanisms tailored to IoT environments.

Future Research Directions:

1. **AI AND MACHINE LEARNING FOR IOT SECURITY** – Future research should explore the integration of AI-driven anomaly detection and predictive analytics to enhance threat detection and response mechanisms. Adaptive AI models that can learn from emerging threats and improve autonomously will be crucial.
2. **SECURE IOT ARCHITECTURES AND PROTOCOLS** – Future studies should focus on designing modular and scalable security architectures, including secure boot mechanisms, hardware-based trusted execution environments, and resilient communication protocols.
3. **ZERO-TRUST SECURITY MODELS FOR IOT** – Implementing and evaluating zero-trust security frameworks tailored for IoT environments could significantly improve security by requiring continuous authentication and strict access controls.
4. **CYBER THREAT INTELLIGENCE SHARING** – Developing frameworks for secure and automated threat intelligence sharing among IoT ecosystems can improve proactive defense mechanisms and enable quicker responses to emerging cyber threats.

By addressing these future research directions, the security and resilience of IoT networks can be significantly enhanced, fostering a more secure and reliable digital ecosystem for the future.

9. REFERENCES

[1] Maglaras, L.A., Ferrag, M. A., Janicke, H., Ayres, N., Tassiulas, L., *Reliability, security, and privacy in power grids*, Computer, 55 (2022b), 85–88.

[2] Reed D., *Applying the OSI seven-layer network model to information security*, SANS GIAC GSEC Practical Assignment Version 1.4 b Option One, 2003.

[3] Kaur D., Singh, P., *Various OSI layer attacks and countermeasure to enhance the performance of WSNs during wormhole attack*, International Journal on Network Security, vol. 5(1), 2014, pp. 62.

[4] Mitrokotsa, A., Rieback, M. R., Tanenbaum, A. S., *Classification of RFID attacks*, Gen,15693, Volume 12, Issue 5, pp. 491–505, 2010.

[5] Li, H., Chen, Y., He, Z., T*he survey of RFID attacks and defenses*, 8th International Conference on Wireless Communications, Shanghai: Networking and Mobile Computing (WiCOM), 2012.

[6] Deogirikar, J., Vidhate, A., *Security attacks in IoT: A survey*, 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, 2017, pp. 32–37, doi: 10.1109/I-SMAC.2017.8058363, 2017.

[7] Sicari, S., Rizzardi, A., Grieco, L., Coen-Porisini, A., *Security, privacy and trust in Internet of Things: The road ahead*, Computer Network, vol. 76, pp. 146–164, Jan. 2015.

[8] Arabo, A., Brown, I., El-Moussa, F., *Privacy in the age of mobility and smart devices in smart homes*, In Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on Social Computing (Social Com). IEEE, 2012, pp. 819–826.

[9] Sarowar, M. G., Kamal, M. S., Dey, N. 2019, *Internet of Things and Its Impacts in Computing Intelligence: A Comprehensive Review – IoT Application for Big Data*, N. Dey and S. Tamane (Eds.), Big Data Analytics for Smart and Connected Cities (pp. 103–136). Hershey, PA: IGI Global. doi: 10.4018/978-1-5225-6207-8.ch005.

[10] Hassanien, A. E., Dey, N., Borra, S. (Eds.), 2018, *Medical Big Data and Internet of Medical Things: Advances, Challenges and Applications*, CRC Press, Boca Raton. eBook ISBN 9781351030380, 2018.

[11] Jelić, A., *What is architecture for? Designing as enriching the landscape of affordances*, Adapt. Behav., vol. 30, no. 6, pp. 585–587, 2022. doi: 10.1177/1059712321994686.

[12] Lu, Y., Cecil, J., *An Internet of Things (IoT)-based collaborative framework for advanced manufacturing*, Int. J. Adv. Manuf. Technol., vol. 84, no. 2, pp. 1141–1152, 2016. doi: 10.1007/s00170-015-7772-0.

[13] Jabraeil, J. M. A., et al., *IoT architecture, in Towards the Internet of Things*, 1st ed. Cham, Switzerland: Springer, 2020, pp. 9–31.

[14] Ahmid M., Kazar, O., *A comprehensive review of the internet of things security*, J. Appl. Secur. Res., vol. 18, no. 3, pp. 289–305, 2023. doi: 10.1080/19361610.2021.1962677.

[15] Alqarawi, G., Alkhalifah, B., Alharbi, N., El Khediri, S., *Internet-of-Things security and vulnerabilities: Case study*, J. Appl. Secur. Res., vol. 18, no. 3, pp. 559–575, 2023. doi: 10.1080/19361610.2022.2031841.

[16] Hassan, A., et al., N*avigating IoT Security: Insights into Architecture, Key Security Features, Attacks, Current Challenges and AI-Driven Solutions Shaping the Future of Connectivity, Computers*, Materials & Continua, 2024, 81(3), 3499–3559.

[17] Alam, T., *Design a blockchain-based middleware layer in the Internet of Things architecture*, Int. J. Informat. Vis., vol. 4, no. 1, pp. 28–31, 2020. doi: 10.30630/joiv.4.1.334.

[18] Gerodimos, A., et al, IoT: Communication protocols and security threats, Internet of Things and Cyber-Physical Systems Volume 3, 2023, Pages 1–13.

[19] Fan, Y., et al., *SNPL: One scheme of securing nodes in IoT perception layer*, Sensors, vol. 20, no. 4, 2020, Art. no. 1090. doi: 10.3390/s20041090.

[20] Rodrigues C. K. D. S., Rocha, V., Towards blockchain for suitable efficiency and data integrity of IoT ecosystem transactions, IEEE Lat. Am. Trans., vol. 19, no. 7, pp. 1199–1206, 2021. doi: 10.1109/TLA.2021.9461849.

[21] Devi M., Majumder, A., S*ide-channel attack in Internet of Things: A survey*, Appl. Internet Things: Proc. ICCCIOT 2020, Singapore, Springer, 2021, pp. 213–222. doi: 10.1007/978-981-15-6198-6_20.

[22] Nasralla, M. M., García-Magariño, I., Lloret, J., *Defenses against perception-layer attacks on IoT smart furniture for impaired people*, IEEE Access, vol. 8, pp. 119795119805, 2020. doi: 10.1109/ACCESS.2020.3004814.

[23] Nebbione, G., Calzarossa, M. C., *Security of IoT application layer protocols: Challenges and findings*, Futur Internet, vol. 12, no. 3, 2020, Art. no. 55. doi: 10.3390/fi12030055.

Cercetări privind utilizarea în siguranță a dispozitivelor inteligente interconectate pe internetul lucrurilor

Internetul lucrurilor (IoT) constituie o rețea global interconectată de dispozitive de calcul, senzori și echipamente de rețea care facilitează schimbul de date prin intermediul unor protocoale de comunicație diverse. Progresele recente în tehnologie au îmbunătățit semnificativ integrarea fără întreruperi a dispozitivelor inteligente. În consecință, alegerea unui design optim de securitate a rețelei este esențială pentru arhitecții de sisteme, necesitând o evaluare atentă a rețelelor nu doar din perspectiva conectivității, ci și a securității. Acest articol prezintă o analiză detaliată a arhitecturii IoT, a securității dispozitivelor și a provocărilor asociate în menținerea cerințelor de securitate pentru dispozitivele IoT. Sunt explorate diverse amenințări cibernetice, mecanismele de atac aferente și strategiile potențiale de atenuare. Mai mult, studiul evidențiază direcții viitoare pentru abordarea provocărilor de securitate ale sistemelor IoT de generație următoare. Scopul empiric al acestei cercetări este de a oferi un rezumat clar al securității IoT, al atacurilor cibernetice și al soluțiilor potențiale, oferind perspective valoroase atât pentru mediul academic, cât și pentru profesioniștii din industrie în contexte diverse.

MANIU Valentin, University of Petroșani /" Nicolae Bălcescu" Land ForcesAcademy, Sibiu, maniu.valentin@armyacademy.ro, 0765948044

PIELE Cosmin University of Petroșani / "Nicolae Bălcescu" Land ForcesAcademy, Sibiu, piele.cosmin@armyacademy.ro