Enhancing Security of Intermediate Devices in the Connection Between IoT Devices and Cloud Service

Damir Regvart*, Miljenko Mikuc**, Luka Zgrablić*, Zlatan Morić*
*Algebra University, Zagreb, Croatia
**University of Zagreb Faculty of Electrical Engineering and Computing, Zagreb, Croatia
damir.regvart@algebra.hr

***Abstract*— The wide spectrum of security challenges, spanning from physical tampering to transport layer vulnerabilities, necessitates a holistic and interdisciplinary strategy. By leveraging existing research while filling up the gaps, this paper seeks to make contributions to the creation of robust security mechanisms. These mechanisms are intended to fortify the IoT ecosystem and ensure the secure transmission of data to the Cloud environment with a specific focus on OSI layers incorporated within network intermediate devices. This paper aims to evaluate the current advancements and identify areas of research within security strategies, protocols, and optimal practices crafted to shield these intermediary components—the physical network devices.**

Keywords—Cloud Security, IoT security, IoT-to-Cloud data traffic, Intermediate devices security .

I. INTRODUCTION

The proliferation of Internet of Things (IoT) devices has brought about a transformative era, redefining the way we interact with our surroundings and manage various aspects of our lives. IoT devices, ranging from smart home appliances to industrial sensors, have seamlessly integrated into our daily routines, enhancing convenience and efficiency. Central to this transformation is the ability of these devices to communicate with cloud platforms, enabling remote monitoring, data analysis, and decision-making. However, as the scope and complexity of IoT ecosystems expand, so do the challenges associated with ensuring the security of communication channels between IoT devices and cloud services [1][2].

The communication between IoT devices and cloud platforms traverses various layers of the OSI model, each susceptible to unique security challenges. From the physical layer to the transport layer, a range of vulnerabilities and threats must be carefully addressed to ensure the integrity, confidentiality, and availability of data and device.

The connection between IoT devices and cloud services often involves a network of intermediate devices that mediate data transmission, data traffic balancing, processing, and storage. These intermediate devices, such as routers, switches, firewalls, and load balancers are responsible in facilitating seamless communication and data flow. While they play a crucial role in enabling the benefits of IoT-to-Cloud convergence, they also present potential vulnerabilities that cyber adversaries would like to exploit.

IoT devices often operate with constrained resources, encompassing limitations in terms of computing power, memory, and energy consumption. Such limitations underscore the need for security mechanisms that are not only robust but also optimized to operate within these resource-constrained environments. This necessitates a departure from traditional security approaches, as solutions must be judiciously designed to strike a balance between protection and resource efficiency.

The diversity of the application domains in which IoT devices are deployed introduce a wide area of distinct security requirements [3]. From industrial automation and healthcare to smart cities and consumer electronics, each domain presents unique challenges and risks. As a result, security mechanisms must be adaptable and flexible, capable of accommodating the specialized demands of each application area while maintaining a cohesive overarching framework.

II. SECURITY CHALLENGES PER OSI LAYER

The Open Systems Interconnection (OSI) model, comprising seven distinct layers, serves as a foundational framework for understanding network communication. Each OSI layer presents unique security challenges that need to be addressed to ensure the overall security and integrity of the network.

As the number of IoT devices continues to grow, the vulnerabilities associated with inadequate security measures become increasingly apparent. Many of these devices are resource-constrained, lacking the computational power and memory required to implement traditional security measures.

TABLE 1 SECURITY ISSUES PER OSI LAYER 1 TO 4

Layer	Issues	Description
Physical layer (Layer 1)	Physical Tampering	Unauthorized physical access to IoT device without physical theft (example: device hardware reset)
	Eavesdropping	Interception of data transmission (data sessions are not adequately protected)
	Radio Frequency Interference	RF interference for communication disruption
	Physical Device Theft	Stolen IoT device can be reverse-engineered or manipulated
Data Link Layer (Layer 2)	MAC Address Spoofing	Attackers could spoof MAC address to gain unauthorized access to the network or impersonate legitime devices
	Man-in-the-Middle Attack	Interception or altering data between IoT devices and gateway
	ARP Spoofing	Manipulation of ARP table to redirect traffic
	Data Frame Manipulation	Attackers can modify or inject malicious content into data frame
Network layer (Layer 3)	IP Spoofing	Attackers can forge IP address to bypass security measures and gain unauthorized access to IoT device
	Routing Attacks	Manipulation of routing table to redirect traffic
	DDoS Attacks	Overwhelming IoT devices or cloud recourses leading to service cut-of or disruption
	DNS attack	Exploit of DNS protocol or service vulnerabilities (availability or stability of the service) or cache poisoning
	Inadequate Firewall Rules	Improperly configured firewalls can allow unauthorized access to IoT devices or cloud service
Transport Layer (Layer 4)	Data Interception	Attackers can intercept and access data during transport if encryption and authentication mechanisms are weak
	Session Hijacking	Attackers can take over established sessions between IoT device and cloud (example: Race condition attacks)
	DoS	Attackers can flood the transport layer with excessive traffic on single or multiple port and make service unavailable
	Traffic Analysis	Unencrypted transport layer data can be analyzed go gather sensitive information about IoT device behavior and users habits
	Protocol Vulnerabilities	Insecure implementation of transport layer protocols can lead to vulnerabilities that attackers can exploit

Main challenges described by [4]-[7] are: data breaches, misconfigurations and inadequate change control, lack of cloud security architecture and strategy, insufficient identity, credential, access and key management, account hijacking insider threats, insecure interfaces and APIs, weak control plane, limited cloud usage visibility, abuse and malicious use of cloud services.

Table I shows current list of main security issues in IoT-to-Cloud data traffic on intermediate devices [11-14]. Layer 1 and Layer 2 issues are mostly common for IoT devices connected to the local network loop, while Layer 3 and Layer 4 are most common ways of a security issues for intermediate devices that are connecting IoT devices to the Cloud service via public Internet or dedicated links.

Intermediate devices, acting as “data intermediaries”, are susceptible to a range of security vulnerabilities. Configuration errors, lack of regular periodic updates, and default credentials might expose these devices to exploitation. Attackers targeting intermediate devices can launch attacks such as traffic interception, unauthorized access, and device compromise. Without proper mechanisms in place, attackers can tamper with data packets, compromising the trustworthiness of the information exchanged between IoT devices and Cloud services [15].

III. LITERATURE REVIEW

In the last decade, there has been a lot of research papers exploring the intricate field of IoT device and cloud service security. These studies have thoroughly investigated the multifaceted landscape, seeking to analyze and understand the various challenges that will surface in this realm. As devices become more prevalent and the range of cloud service options expands, coupled with the complexity of communication protocols and application domains, the security paradigm has become increasingly complicated.

A. Methodology for literature review

A comprehensive literature review was conducted, encompassing the evaluation of recent research articles. Google Scholar [16] was employed as the primary tool, employing targeted keywords: "*Cloud security*" in conjunction with "*IoT security*", filtered through the lens of

OSI layers, research gaps and state of the art with cross-checking given citations and paper references.

This search spanned research papers published between 2018 and May 1st, 2023, with a distinctive focus on categorizing the OSI layer each paper addressed as a organized structure. Reviewing scientific articles from the past five years guaranteed access to the latest information, emerging trends and also sidestepping redundancy and increasing relevance to contemporary issues within the field topic. Some relevant papers before 2018 were included and relevant updates to the research topic were also included. To streamline the research workflow for the literature review, the AI Research Assistant *Elicit* [17] was also included, introducing an automated dimension to the process. Within these papers, categorized in Table II, a consistent unifying theme emerges—a focus on the distinctive security challenges arising from the inherent heterogeneity of IoT devices and the extensive array of cloud services. Some of the articles outweigh multiple layers of a whole layer architecture so some of the row articles can also be found in other rows of the table. Articles were also sorted and selected based on repetends, citations and author subject interest.

TABLE II. LITERATURE REVIEW

OSI layer	**Research papers**	
	Google Schoolar (since 2018):	***Selected papers:***
Layer 1+2	902	8
Layer 3+4	1010	16
Layer 1->4	864	12
Upper Layers	986	9

Research papers have embarked on the task of solving these challenges [18], identifying vulnerabilities that punctuate cloud ecosystems and IoT devices.

B. Grouped OSI multilayer Security issues

1) Security Issues at the Physical and Data Link Layers

Studies have highlighted the criticality of securing the physical and data link layers in the context of IoT communications. Attack vectors such as MAC address spoofing, unauthorized physical access, and signal interception pose substantial threats. Studies have emphasized the importance of physical security measures, such as tamper-evident packaging and hardware-based authentication, to deter unauthorized physical access [19].

2) Security Challenges at the Network and Transport Layers

The network and transport layers emerge as focal points for security concerns due to their pivotal roles in routing, addressing, and data transmission. Multiple research articles have highlighted the vulnerabilities of routing protocols to attacks like black-holing, sinkhole, and Sybil attacks [20]. To address these challenges, novel secure routing protocols have been proposed, incorporating authentication and anomaly detection mechanisms. Furthermore, concerns related to IP address spoofing, session hijacking, and transport layer attacks have prompted investigations into adaptive security mechanisms, enhanced session management techniques, and secure transport protocols.

3) Cross-Layer Approaches and Integrated Solutions

The literature shows a growing trend towards cross-layer approaches that leverage the synergistic benefits of multiple OSI model layers. Studies have proposed integrated security solutions that combine physical layer encryption, data link layer authentication, and network layer anomaly detection. These approaches aim to create a holistic security framework that addresses vulnerabilities across different layers and ensures comprehensive protection against attacks [21]. Unlike traditional security methods that operate in isolation at specific OSI layers, cross-layer approaches transcend these boundaries, orchestrating collaboration and information sharing between different layers.

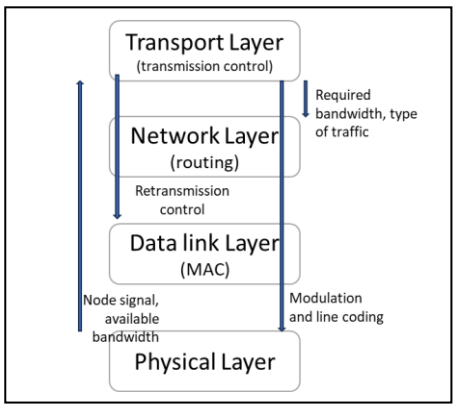

Figure 1. Simple OSI cross-layer architecture

Cross-layer approaches (shown in Fig. 1) have emerged as a pivotal strategy in addressing the multifaceted security challenges inherent in the connection between IoT devices and cloud services. By harnessing the synergistic potential of cross-layer interactions, security mechanisms can adapt dynamically to evolving threats and vulnerabilities by integrating multiple security mechanisms, such as encryption, authentication, intrusion detection, and access control [22].

IV. FUTURE RESEARCH DIRECTIONS

Regarding the literature review several topics are open for future study:

- Adaptive AI-Driven Security
- Privacy-Preserving Mechanisms
- Blockchain for IoT Security data transfer
- Quantum-Resistant Security
- Collaborative Security Ecosystems

A. Adaptive AI-Driven Security

Integration of artificial intelligence and machine learning techniques for real-time threat detection, behavioral analysis, and anomaly identification holds significant promise. Developing AI-driven adaptive security mechanisms [23] that learn from IoT device behaviors can enhance detection accuracy while minimizing false positives.

This technique includes following areas:

- Active monitoring - Continuous 24/7 overwatch the network and system activities in real-time,
- Dynamic Adaptation - As the AI algorithms learn from new data, they adapt and refine their understanding of what constitutes normal behavior and potential threats
- Automated Response - AI system can automatically trigger responses on threat detection
- Behavioral Analysis - AI focus on utilizing how the system is being used and how it interact with the network
- Threat Intelligence Integration - continuous input from external databases as a emerging learning method integrated with active monitoring

While Adaptive AI-Driven Security for the network traffic offers a promising approach to bolstering network defenses, challenges such as false positives, interpretation of the data, the need for extensive training data, and potential adversarial attacks on AI models must be addressed.

B. Privacy-Preserving Mechanisms

This method includes protecting user data privacy while enabling data transfer analysis. Differential privacy, secure aggregation, and homomorphic encryption are areas open for research work.

Key characteristics of privacy-preserving mechanisms include [24][25]:

- Data Encryption - fundamental privacy-preserving technique
- Data Anonymization - removing or altering personally identifiable information from data sets to make it difficult to link data to specific individuals.
- Differential Privacy - "mathematical" framework that introduces controlled noise or randomness into the data to ensure that individual contributions cannot be uniquely identified.
- Homomorphic Encryption - allows computations to be performed on encrypted data without decrypting it first.
- Secure Multiparty Computation - allows multiple parties to jointly compute a function over their individual private inputs without revealing those inputs to each other.
- Tokenization - involves replacing sensitive data with unique tokens or references while storing the actual data securely in a separate location.
- Privacy-Preserving Protocols - upgrade of data encryption that ensure that data interactions and user identity are protected while still enabling secure communication and authentication.
- Data Minimization - only minimal data collection will be retained thrust reducing the risk for user privacy.

Privacy-preserving mechanisms offer numerous benefits by safeguarding sensitive data and enabling compliant data sharing. However, they also introduce noise and trade-offs with potential challenges to IoT-to-Cloud traffic between **data privacy and usability**, and it is a possible area that can be adequately addressed within the multidisciplinary study.

C. Blockchain for IoT Security

Blockchain technology is decentralized and tamper resistant. The nature of blockchain technology presents intriguing possibilities for enhancing data transfer integrity. Blockchain enables IoT device owners to control and monetize their data by securely sharing it with authorized parties in exchange for value, all while maintaining their privacy and data ownership [26].

The benefits of blockchain stated in articles [24-26] are:

- Enhanced Data Integrity - each data point, once added to the blockchain, becomes a permanent part of the historical record, ensuring the authenticity and trustworthiness of the information;
- Secure Identity Management - each device is assigned a unique identifier, and its interactions can be traced transparently;
- Immutable Auditing and Compliance - trail of events is created with each new data point;
- Decentralized Access Control - validation of the data and data point can be done without the need of “central” point;
- Data Sharing and Monetization - while the data is “secured” (not tampered) the same data has a value and its sharing can be limited or monetized.

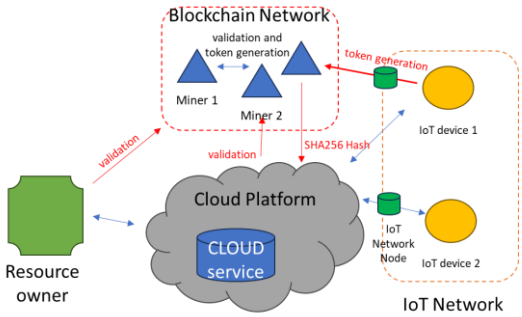

Figure 2. Blockchain IoT architecture

The decentralized structure of blockchain negates the necessity for a central governing body as shown in Fig. 2, effectively diminishing vulnerabilities arising from singular points of control. In the realm of IoT security, blockchain emerges as an auspicious remedy to elevate the safety of interactions among IoT devices, cloud services, and other interconnected entities.

D. Quantum-Resistant Security

Quantum based computing is a emerging field of research work. Research into quantum-resistant cryptographic techniques is crucial to ensuring that IoT-to-Cloud security measures remain effective in the face of future emerging threats [27].

Current research areas:

- Post-Quantum Cryptography - replacing current encryption and digital signature algorithms with alternatives that are resistant to quantum attacks;
- Quantum Key Distribution (QKD) - secure key exchange between parties and utilizing physical properties of quantum state of light for detecting possible eavesdropping [28];
- Hash/Code-Based Cryptography - enhancement of current cryptography methods.
- Migration Strategies for quantum network - various research on how-to transition from current cryptographic protocols to new quantum-resistant ones without compromising security [29];
- Standardization Efforts - embracing development of quantum-resistant security in regards to interoperability and adoption of new protocols and methods.

While the full impact of quantum computing on cybersecurity remains uncertain, investing in quantum-resistant security could ensure that sensitive information remains protected against emerging threats posed by quantum computers when they become accessible. The current costs of associated research must also be included.

E. Collaborative Security Ecosystems

Benefit from collaborative security ecosystem is that in the event of a cyber incident, collaborative ecosystems enable coordinated incident response efforts. Potential challenges and negative aspects associated with collaborative security ecosystem can be overcome by addressing negative aspects that may include thrust and reputation, national regulation challenges, intellectual right management, false pozitive overload, lack of skills.

Examples of collaborative security ecosystems include Information Sharing and Analysis Centers (ISACs) [30], industry-specific forums, threat intelligence sharing platforms [31], and public-private partnerships focused on cybersecurity.

V. Conclusion

Secure communication between IoT devices and the cloud is not just a technological challenge but an imperative for building trust, sustaining innovation, and safeguarding user experiences. The insights gained from this study underscore the dynamic and evolving nature of IoT security challenges and the need for adaptable, multi-layer security strategies [32].

By identifying vulnerabilities spanning the layers of the OSI model and harnessing the combined capabilities of integrated solutions, the IoT ecosystem can progress towards fully embracing connectivity's potential while minimizing inherent risks. This paper aims to enrich the ongoing research topics surrounding IoT-to-Cloud security and motivate forthcoming endeavors dedicated to establishing a secure and robust IoT environment concerning data transmission to the Cloud through intermediate network devices.

The key findings in literature review can be summarized as:

- **Identification of vulnerabilities** in intermediate devices: A thorough analysis of the vulnerabilities present in these devices revealed potential points of compromise that could lead to data breaches and unauthorized access [33].
- **Exploration of network and transport layer threats**: The examination of threats at these layers exposed the range of risks, from routing attacks to vulnerabilities in communication protocols.
- **Examination of security mechanisms**: The study has delved into various security mechanisms, including encryption protocols, network segmentation, and intrusion detection systems, providing a comprehensive toolkit for mitigating security challenges [34].
- **Multidisciplinary approach**:The multidisciplinary perspective adopted throughout this paper underscores the interconnectedness of networking, cybersecurity, and IoT technology in devising robust security solutions.

This paper highlights certain research areas that merit further exploration. The integration of artificial intelligence and machine learning techniques for anomaly detection and behavior analysis across OSI layers is one such area. Additionally, while many studies focus on individual layers,

there is a need for more research that examines the interplay between different layers and their combined impact on security.

REFERENCES

[1] J. Singh, T. Pasquier, J. Bacon, H. Ko and D. Eyers, "Twenty Security Considerations for Cloud-Supported Internet of Things," in IEEE Internet of Things Journal, vol. 3, no. 3, pp. 269-284, June 2016, doi: 10.1109/JIOT.2015.2460333

[2] Tawalbeh, Lo'ai, Fadi Muheidat, Mais Tawalbeh, and Muhannad Quwaider. 2020. "IoT Privacy and Security: Challenges and Solutions" Applied Sciences 10, no. 12: 4102. https://doi.org/10.3390/app10124102

[3] Pallavi Sethi, Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications", Journal of Electrical and Computer Engineering, vol. 2017, Article ID 9324035, 25 pages, 2017. https://doi.org/10.1155/2017/9324035

[4] Singh, A., & Chatterjee, K. (2017, February 1). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications. Academic Press. https://doi.org/10.1016/j.jnca.2016.11.027

[5] S. H. L. Kanickam, L. Jayasimman and A. N. Jebaseeli, "A Survey on Layer Wise Issues and Challenges in Cloud Security," 2017 World Congress on Computing and Communication Technologies (WCCCT), Tiruchirappalli, India, 2017, pp. 168-171, doi: 10.1109/WCCCT.2016.49.

[6] I. Butun, P. Österberg and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 616-644, Firstquarter 2020, doi: 10.1109/COMST.2019.2953364.

[7] Liu, Y., Chen, H. H., & Wang, L. (2017). Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges. IEEE Communications Surveys and Tutorials, 19(1), 347–376. https://doi.org/10.1109/COMST.2016.2598968

[8] Wu, Y., Khisti, A., Xiao, C., Caire, G., Wong, K. K., & Gao, X. (2018). A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead. IEEE Journal on Selected Areas in Communications, 36(4), 679–695. https://doi.org/10.1109/JSAC.2018.2825560

[9] Rahman, R. A., & Shah, B. (2016). Security analysis of IoT protocols: A focus in CoAP. In 2016 3rd MEC International Conference on Big Data and Smart City, ICBDSC 2016 (pp. 172–178). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICBDSC.2016.7460363

[10] Tewari, A., & Gupta, B. B. (2020). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future Generation Computer Systems, 108, 909–920. https://doi.org/10.1016/j.future.2018.04.027

[11] Mitseva, A., Panchenko, A., & Engel, T. (2018, June 1). The state of affairs in BGP security: A survey of attacks and defenses. Computer Communications. Elsevier B.V. https://doi.org/10.1016/j.comcom.2018.04.013

[12] Sanjuan, E. B., Cardiel, I. A., Cerrada, J. A., & Cerrada, C. (2020). Message Queuing Telemetry Transport (MQTT) Security: A Cryptographic Smart Card Approach. IEEE Access, 8, 115051–115062. https://doi.org/10.1109/ACCESS.2020.3003998

[13] Jangjou, M., & Sohrabi, M. K. (2022, October 1). A Comprehensive Survey on Security Challenges in Different Network Layers in Cloud Computing. Archives of Computational Methods in Engineering. Springer Science and Business Media B.V. https://doi.org/10.1007/s11831-022-09708-9

[14] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006

[15] Google Schoolar, https://scholar.google.com/

[16] Elicit, https://elicit.org/

[17] Balogh, Stefan et al. "IoT Security Challenges: Cloud and Blockchain, Postquantum Cryptography, and Evolutionary Techniques." Electronics (2021): n. Pag.

[18] Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 78, 680–698. https://doi.org/10.1016/j.future.2016.11.009

[19] Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016, September 1). A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. Proceedings of the IEEE. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/JPROC.2016.2558521

[20] Mrabet, Hichem, Sana Belguith, Adeeb Alhomoud, and Abderrazak Jemai. 2020. "A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis" Sensors 20, no. 13: 3625. https://doi.org/10.3390/s20133625

[21] Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H., & Tang, Y. (2018). Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. Journal of Network and Computer Applications, 106, 117–123. https://doi.org/10.1016/j.jnca.2018.01.003

[22] Nassif, A. B., Talib, M. A., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine Learning for Cloud Security: A Systematic Review. IEEE Access. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2021.3054129

[23] S. Rangaraju (2023). Secure by Intelligence: Enhancing products with AI-Driven security measures, EPH - International Journal of Science And Engineering, vol. 9, no. 3. Green Publication, pp. 36–41, Dec. 01, 2023. https://doi.org/10.53555/ephijse.v9i3.212.

[24] Zhang, J., Chen, B., Zhao, Y., Cheng, X., & Hu, F. (2018). Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues. IEEE Access, 6, 18209–18237. https://doi.org/10.1109/ACCESS.2018.2820162

[25] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems, 88, 173–190. https://doi.org/10.1016/j.future.2018.05.046

[26] Fernandez-Carames, T. M. (2020, July 1). From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things. IEEE Internet of Things Journal. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/JIOT.2019.2958788

[27] Wang, L. J., Zhang, K. Y., Wang, J. Y., Cheng, J., Yang, Y. H., Tang, S. B., Pan, J. W. (2021). Experimental authentication of quantum key distribution with post-quantum cryptography. Npj Quantum Information, 7(1). https://doi.org/10.1038/s41534-021-00400-7

[28] https://www.nationalisacs.org/

[29] Brijwan & others. Future of Quantum Computing in Cyber Security. In Handbook of Research on Quantum Computing for Smart Environments, 2023. https://doi.org/10.4018/978-1-6684-6697-1.ch016

[30] https://www.misp-project.org/

[31] Li, S., Tryfonas, T., & Li, H. (2016). The Internet of Things: a security point of view. Internet Research, 26(2), 337–359. https://doi.org/10.1108/IntR-07-2014-0173

[32] Li, S., Tryfonas, T., & Li, H. (2016). The Internet of Things: a security point of view. Internet Research, 26(2), 337–359. https://doi.org/10.1108/IntR-07-2014-0173

[33] Dong, Z. C., Tian, M., & Ding, L. (2021). A framework for modelingand structural vulnerability analysis of spatial cyber-physical powerpystems from an attack–defense perspective. IEEE Systems Journal, 15(1),1369–1380

[34] A. Cirne, P. R. Sousa, J. S. Resende, and L. Antunes. IoT security certifications: Challenges and potential approaches. Computers & Security, vol. 116. Elsevier BV, p. 102669, May 2022. doi: 10.1016/j.cose.2022.102669.