Journal of Applied Artificial Intelligence
https://jaai.sabapub.com
ISSN: 2709-5908

2023 Volume 4, Issue 2: 12-21

DOI: https://doi.org/10.48185/jaai.v4i2.920

A Comprehensive Analysis of Cybersecurity Threats based IoTs

Fatina Shukur[1, *], Sinan T. Shukur[2]

[1] Faculty of Computer Science and Mathematics, University of Kufa, Al-Najaf, Iraq

[2] Faculty of Medicine, University of Kufa, Al-Najaf, Iraq

Received: 03.11.2023 • Accepted: 26.12.2023 • Published: 28.12.2023 • Final Version: 28.12.2023

Abstract: The rapid growth of the Internet of Things (IoT) in our daily activities, has led to serious concerns regarding to potential cybersecurity threats. Therefore, there is a real need to have active and proactive solutions. This research undertakes an extensive analysis review of literature for the existing cybersecurity challenges and threats within various IoT devices. Also, it presents the suggested solutions as well as the structural frameworks. Moreover, it helps to detect and identify possible threats using different methods. Furthermore, it makes a contribution by drawing attention to research gaps within industrial and economic fields based IoTs. According to our findings, the main concern issues in IoT systems are cybercrimes and privacy cases. Artificial Intelligence, on the other hand, presents promising opportunities to improve cybersecurity. Nonetheless, certain attacks including authentication and confidentiality remain unaddressed when applying current solutions. This is, in fact, calling for more investigation and practical testing of suggested defences.

Keywords: Internet of Things, Cybersecurity, Threats and Risks.

1. Introduction

The Internet of Things (IoT) has penetrated many important fields, such as the medical, educational, and financial fields. Nonetheless, the Internet of Things is used largely at homes, offices, streets, big cities, etc. All of which are as significant. Furthermore, the IoT facilitates connectivity to intelligent things, cloud services, and different applications. In 2020, there were 50 billion devices based IoT mechanism connected online [1], each of which is generated massive source of data. Also, the world has rapidly grown to rely on artificial intelligence, which is a growing trend in the digital world. As a result, manufactures and IoT designers are under pressure to protect this technology so that they can fulfil future needs with high demands.

Trusting an IoT device begins by proving its security. This is an essential step, particularly when such device is connected to the internet. This connection makes it vulnerable to numerous security risks such as software privacy, harmful assaults, cyber and malware attacks [2]. However, the ongoing need for improvement and updating in this area can not rely on existing methods to ensure security. With

[*] Corresponding Author: fatinat.shukur@uokufa.edu.iq

new threats regularly emerging, it is necessary to continually update existing frameworks and propose new solutions while also updating IoT fields.

Therefore, conduct a regular review of the applicable techniques is high recommended. Thus, this research proposes the analysis of the latest advancements of different types of cybersecurity threats based IoT technology as well as the problems its devices face. This study also highlights various cybersecurity frameworks and methodologies which are proposed for cybersecurity in the IoT field.

2. Research Problem

The characteristics of the IoTs, including its numerous system connections and handling of massive volumes of data, have made it more likely that hackers will target it. Furthermore, vendors are not the only parties with concerns about IoT cybersecurity, but consumers need technology that they could trust [6]. The best security solutions for this developing technology are desperately needed [31]. Nonetheless, the range of suggested methods and proposed solutions which were given by the latest research on IoT cybersecurity has prompted the following queries. Which methods have proven to be most effective in identifying IoT vulnerability? Which new developments are we seeing in IoT cybersecurity? Which types of attacks can target the IoTs systems?

3. Motivation, Aim, and Objective

As we enter a new phase of technological advancements with virtual reality, the possibilities for the Internet of Things (IoT) are limitless. The IoT is experiencing rapid growth and is recognised as a transformative force in technology and artificial intelligence. The usage of IoT devices is expanding exponentially, demonstrating their profound influence on various industries [4].

Although the IoTs will soon revolutionise the world, risk management experts are concerned about the IoT's privacy and cybersecurity. These issues are given top priorities. Nevertheless, if security challenges, such as confidentiality and privacy, are adequately addressed, IoT will entirely transform everything [5]. A comprehensive risk management plan for the IoT is necessary, with an emphasize on cybersecurity challenges, due to the massive data generated from interacting with IoT devices on a daily basis. These data are highly sensitive to risk attacks.

This research is *motivated* by a real need to address the growing cybersecurity risks which are associated with IoT technologies/devices. Since cyberattacks are becoming more common and complex, we need to investigate deeply and closely at all of the many kinds of potential risks that are affecting IoT technologies/systems.

The *aim* of this research is to present a through overview of the state of IoT cybersecurity risks including threats and difficulties. We will be exploring the body of current literature and learning from earlier research. In order to strengthen IoT security, this study aims to provide a point of reference for academics, decision makers, and business professionals.

Through our analysis of the framework and detection methods that have been proposed in the literature, we hope to uncover possible paths towards improving IoT ecosystem protection. In addition, the review will highlight any research gaps that currently exist and provide guidance for upcoming studies and advancement in IoT cybersecurity area of research.

The principal *objective* of this research is to synthesise and provide a coherent literature review that indicate the most common attacks and problems while also offering insightful information about the suggested solutions and how well they would work. Also, this research will provide an extensive analysis that adds to the expanding knowledge based IoT cybersecurity. Moreover, it emphasises on finding and defining the most vulnerable areas of IoT security.

Furthermore, this study will increase awareness of the significance of strong cybersecurity measures that embedded with IoT devices as well as the overall systems. This is by highlighting the importance of IoT security, in addition to mitigate the possible risks and threats.

The overall goal of this review is to promote a safer and more resilient environment of IoT systems. Thus, researchers can develop further and prosper in this field despite new cyberthreats.

4. Literature Review

This section offers a critical review of the most significant research on IoT cybersecurity that has been done by academics, with a particular emphasis on studies that have been published during the last ten years.

Research [1] highlighted the significance of focusing on the two primary risks which, in fact, impair the IoT. These include malware attacks and software piracy. This research employed an empirical methodology, with experiments that carried out to validate the suggested solutions. On the other hand, the research's goal was to present a novel method to solving the problem by identifying files infected with malware and pirated software throughout the IoTs. Also, the experimental results demonstrated that the novel solution method that was suggested performs better in terms of IoT cybersecurity than the earlier methods.

According to research [2], the IoT is becoming much more integrated into our daily activities, in which, it is associated with many different risks by its nature. This empirical research carried out a risk analysis to find vulnerabilities within IoT architecture. The principal goal of the research was to determine the most important security risk that IoT application faces and that a developer would be aware of in order to ensure its security. Its main findings demonstrated that, depending on the given situation, intelligent switches, sensors, and tiny actuators are the most susceptible components of IoTs.

Assessment of IoT risk principles were described in research [3]. This study's primary goal was to determine why the risk evaluation techniques used today for the IoTs are insufficient. Its findings indicated the following as the primary causes of the insufficiency of the IoTs risk evaluation methods. Limitation in the understanding of systems, shifting boundaries within systems; deficiencies in periodic evaluation; the difficulty of comprehending the indirect threats; and neglecting to view assets as a platform for attacks. Also, it was necessary to develop new mechanisms to simulate predictive powers, in addition to have automated risks evaluation methods.

A research survey in [5] covered the IoT's current state and its obstacles. The research's primary objective was to present an overview of security principals, challenges, and upcoming developments within IoT security. An extensive review of relevant literature served as the foundation for the methodology employed by the writers. Their findings demonstrated that existing research of the IoTs focused on access verification as well as control protocols.

Research [7] focused on cybersecurity risks associated with healthcare sectors, specially to IoT based hospitals and clinics services. It presented a framework for adaptive cybersecurity that can automatically respond to online threats. The research concentrated on developing cutting-edge adaptive security solutions that foresee and counteract adaptive attacks directed against infrastructures and healthcare facilities. According to the findings, the framework successfully defended against presented attacks.

The IoT's privacy concerns were investigated in [8], along with how cybersecurity and computational intelligence could possibly work together. The research's goal was to find out the viability of applying computational intelligence tools and methods to address the IoT cybersecurity problems. Data for this study was gathered through the review of relevant literature. This research's primary contribution was to draw attention to the difficulties that computational intelligence methods have within IoTs.

Another research in [9] discussed the urgent requirement for innovative approaches to counteract cybercrimes that are affecting IoT systems around the world. Authors presented their opinions, experiences, and suggestions on how to stop cybercrimes. The primary contribution of this research was to present an extensive overview of different challenges based IoT cybersecurity. It suggested blockchain as the perfect solution providing integrity and encryption.

A classification of the various threats that impact IoT systems, in addition to examination of intrusions and attacks, were the objectives of research [10]. The findings indicated that when it came to IoT cybersecurity, concerns such as privacy and confidentiality were of the utmost importance. Also, the study helped other researchers to do a deep investigation that focus more on the effect of privacy and confidentiality threats.

Authors in [11] addressed the problem of user information theft because they believe that IoT system is extremely susceptible to these kinds of problems. The article aimed to improve the progress of IoT research by concentrating on diverse IoT security challenges, in addition to highlight the existing proposed solutions. It covered different attacks such as z-wave, network, and physical attacks. Although main findings of existing solutions are application security and secure communication protocols, authors suggested to use a digital signature because of the nature of IoT components.

An analysis of IoT users' ignorance of its risks, particularly those related to data loss and misuse, was covered in research [12]. Since the paper was a review, the authors extracted information they needed from other studies that had already been published. The article was restricted to non-manufacturer-supported devices. Various attacks with different categories have been identified. Moreover, the study demonstrated that inadequate security has raised serious concerns about a skilled attacker could take advantage of ecosystem vulnerabilities.

5. Existing Solutions

Research [15] looked into a review about cybersecurity incident response within IoT systems that used in intelligent applications. Its goal was to improve the cybersecurity evaluation model for IoT in such environment. The suggested model considered improvement of cybersecurity within an intelligent environment. It recommended the integration of supplementary methodologies to increase its performance.

In accordance with global regulations, research [16] presented developing reliable healthcare services within IoTs. This work is comparable to a case study because its methodology involved creating the superior security assurance, in addition to create a hierarchical cybersecurity strategy. This research's primary objective was to create a real IoT architecture-based healthcare system. One of the main outcomes was a comprehensive model that demonstrate the security of each layer, while producing results that are verifiable and traceable to all parties involved.

The research [17] covered the security issues related to the incorporation of industrial control systems within IoT field. The goal of the empirical research was to present a new model for verifying control systems' security at the outset of their design. The model's ability in recognising and alleviating possible cyberthreats was shown in experimental cases as well as improve its security.

Research [18] has reviewed how mobile computing technology is applied to protect the IoT. It presented a comprehensive analysis of the key problems and challenges of IoT devices cybersecurity in the context of mobile computing. The article's primary findings demonstrated that IoT-based devices are vulnerable to different ranges of attacks. Therefore, strong security measures are advised to enhance their cybersecurity. Preferably, the proposed measures can use mobile computing mechanism so that it addresses both software as well as hardware security domains. As a result, researchers within cybersecurity community will concentrate on mobile computing as a key element of this discipline.

6. Future Possible Directions

Artificial Intelligence (AI) may be able to help with the cybersecurity issues brought by the IoTs [4]. It determines the main issues and suggested methods by applying artificial intelligence to improve security in IoTs. The article outlined the necessity of ongoing AI techniques development, in addition to highlight intents underlined cyberattacks which belong to AI and IoT together. Moreover, it provided cybersecurity professionals with practical mechanisms for safeguarding IoT networks and promoting a more secure overall system.

In view of the growing usage of IoT devices globally, research [6] covered cybersecurity concerns raised by suppliers and customers. Two cases attacks were tested using review information of relevant literature. This research's primary objectives were to list the most popular IoT applications, in addition to assess the problems that will affect cybersecurity going forward. The research's findings demonstrated that the evaluated cases exposed the IoT systems' high level of vulnerability.

In research [20], security issues were discussed in companies that use a lot of IoT as well as information systems. It stressed how crucial it is to manage risks effectively as they can mostly be existed. The research determined that the existing methods for assessing risk of information security are inadequate. Therefore, an advanced method has been proposed to evaluate the risks in a small scale of IoT environment. Although the suggested method is only applicable to one specific environment, its simulation experiment has shown its effectiveness.

Using IoT devices in smart homes can lead to privacy violations, as highlighted in [21]. It suggested a strategy to assist end users who are not familiar with IoT risks in identifying, evaluating, and effectively mitigating these risks. A survey gathered existing risks approaches. The constraint is the exclusive emphasis on household devices. The results presented the users with important information and awareness to help them making a wise choice with their home, in addition to be aware of potential risks.

The fast adoption of IoT and cyber based physical systems, which has led to various security concerns, was presented in [24]. The research's primary goals were to identify the security vulnerabilities in the available IoT devices. Also, create minimum cost security mechanisms for IoT systems. Industrial as well as commercial cases have been considered in this research. Significant findings indicated that both cases had a high level of attacks susceptibility. Thus, better alternative solutions were required as IoT devices with their different applications are becoming widely used in the coming years.

7. Analysis, Results and Discussion

This section presents and analyses the outcomes/ suggested solutions of previous studies. Numerous IoT threats have been covered by the literature of these studies. Their contents differed and presented different categories that affected by different factors; some have concentrated on particular attacks, while others outlined the suggested methodology; drawn a structure framework; or discussed more general IoT security challenges. These threats categories with their proposed solutions and results include the following, in which the following table shows the comparative analysis factors for some of them.

Table 1. Comparative analysis factors of IoTs threats.

Article	Attacks Factors	Proposed Solutions
[1]	Malware and software privacy	• A method to search the IoT network for files which could contain malware and software that have been illegally downloaded. • The deep neural network TensorFlow is used to identify software that has been pirated. • Eliminate noisy data by using weighting and tokenization features.
[2]	Confidentiality issues and information exploitation	EBIOS methodology is applied to analyse possible risks.
[7]	Attacks on healthcare services	Framework based dynamic adaptive cybersecurity.
[8]	Malware identification, vulnerability of IoT systems, and issues of data security and personal safety	Cyber defences based artificial intelligence along with privacy preserving data approach, in addition to use 5G IoT architecture.
[9]	Cybercrimes' effects on the world economy	Apply blockchain mechanism.
[15]	Cybersecurity hackers can target water and electricity infrastructure, they take control on smart cities, and bring them down	A methodology to assess IoT cybersecurity which is applied in smart cities.
[17]	Fake attacks, disclosure private information	Applied a suggested framework for industrial security system verification.
[21]	Privacy violations	Used mobile application to check quickly and instantly the security status of IoT-enabled household devices.

Keeping a self-control of a smart city is a challenge issue. Cybersecurity hackers may target the water and electricity infrastructure that causing daily necessities to collapse [15]. Continuing with the same field, privacy breaches targeting a smart home had an effect on the world physically [21]. Furthermore, as noted by [22], the security of smart homes can be compromised by network or physical attacks, in addition to network routing issues and service stability [26]. Safeguarding homes methodologies and mobile applications were the suggested solutions for such attacks.

Attacking cybersecurity raised concerns about the effects on the industrial devices, as well as the whole economy. Therefore, the next impact of economy would be the cybersecurity. IoTs based industrial devices were extensively utilised [19, 23, 24, 27]. Mapping the relationship between different IoT devices components was used to calculate the economic impact.

The previous studies addressed the threat posed by cybersecurity attacks to healthcare services, which included physical attacks, in addition to data loss [7, 16]. Also, the health sector has been negatively impacted by cyberattacks. One of the suggested solutions was to use hierarchical standards of international cybersecurity, as well as apply the dynamic mechanism of cyber threats.

A lot of academics were also interested in the topic of cybercrimes, which was a major concern and important area of research [3, 9, 12, 29]. Cyberattacks affected the world economy, the resources of organisations, personal data profiling, as well as private information. The human factor approach to get cybersecurity profiles, and blockchain technology were among the suggest approaches.

Privacy concerns were a significant issue that were covered in earlier research [6, 8, 10, 11, 13, 14, 17, 18, 20, 25, 28]. These concerns include theft, identity spoofing, access to the private and personal information. Suggested solutions could be a risk prediction approaches, software and hardware protections, and cyber defences based intelligent techniques. Results in [8, 9, 10, 12, 21, 28, 29] showed the top privacy concerns were related to IoT cybersecurity and cybercrime.

By our reviewing the previous literature, it can be notified that machine learning approaches did not apply deeply within IoT cybersecurity framework. Identification and description of their roles is necessary to be improved. Additionally, some attacks remain unaddressed well by the given solutions. Therefore, in line with the viewpoints of [9, 22], we suggest conducting a further and deep research by applying real-world scenarios to verify the efficiency of each of these given solutions. Such attacks could include confidentiality, authentication, and networking of data server [30].

8. Conclusion

This comprehensive analysis has clarified the complexity and dynamic field of IoT cybersecurity system. The overall aim of this study is to promote a safer and more resilient environment of IoT systems. This literature review showed that IoT systems are vulnerable to a variety of cyberthreats. Moreover, privacy cases and cybercrimes are emerging to be the primary threats. Although these results are in line with existing knowledge, they emphasise of the importance to keep working within this area of research to address or mitigate these issues. In addition, this study suggested the use of artificial intelligence tools to improve the IoT cybersecurity systems. With increasing the complexity and capacity of IoT ecosystem, traditional cybersecurity mechanisms might not be enough to defeat sophisticated attacks.

Although, the review offered insightful information about the body of current IoT cybersecurity research, there are many essential areas that require more investigation. This research indicated that certain attacks were not fully addressed by the suggested solutions. Hence, some real-world scenarios need more deep and further investigations with specialised strategies. Future directions should therefore concentrate on multidisciplinary collaboration as well as apply cutting-edge technologies.

IoT cybersecurity field needs continuous attention to details in order to effectively defend cyber threats in such dynamic environment. This review can be considered as a solid foundation for further research to undertake. Researchers can work together as a team to create a more secure IoT system. Consequently, they can develop further and prosper in this field despite new cyberthreats.

References

[1] Ullah, F.; Naeem, H.; Jabbar, S.; Khalid, S.; Latif, M.A.; Al-Turjman, F.; Mostarda, L. Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach. IEEE Access 2019, 7, 124379–124389.

[2] Zahra, B.F.; Abdelhamid, B. Risk Analysis in Internet of Things Using EBIOS. In Proceedings of the 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Vegas, NV, USA, 9–11 January 2017; pp. 1–7.

[3] Nurse, J.R.C.; Creese, S.; De Roure, D. Security Risk Assessment in Internet of Things Systems. IT Prof. 2017, 19, 20–26.

[4] Kuzlu, M.; Fair, C.; Guler, O. Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. Discov. Internet Things , 2021, 1, 7.

[5] Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015; pp. 336–341.

[6] Tweneboah-Koduah, S.; Skouby, K.E.; Tadayoni, R. Cyber Security Threats to IoT Applications and Service Domains. Wirel. Pers. Commun. 2017, 95, 169–185.

[7] Boudko, S.; Abie, H. Adaptive Cybersecurity Framework for Healthcare Internet of Things. In Proceedings of the 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), Oslo, Norway, 8–10 May 2019; pp. 1–6.

[8] Zhao, S.; Li, S.; Qi, L.; Da Xu, L. Computational Intelligence Enabled Cybersecurity for the Internet of Things. IEEE Trans. Emerg. Top. Comput. Intell. 2020, 4, 666–674.

[9] Abdullah, A.; Hamad, R.; Abdulrahman, M.; Moala, H.; Elkhediri, S. CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 1–3 May 2019; pp. 1–6.

[10] Abomhara, M.; Køien, G.M. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. J. Cyber Secur. Mobil. 2015, 4, 65–88.

[11] Islam, M.R.; Aktheruzzaman, K.M. An Analysis of Cybersecurity Attacks against Internet of Things and Security Solutions. J. Comput. Commun. 2020, 8, 11–25.

[12] Gurunath, R.; Agarwal, M.; Nandi, A.; Samanta, D. An Overview: Security Issue in IoT Network. In Proceedings of the 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 30–31 August 2018; pp. 104–107.

[13] Atlam, H.F.; Wills, G.B. An efficient security risk estimation technique for Risk-based access control model for IoT. Internet Things 2019, 6, 100052.

[14] Strecker, S.; Van Haaften, W.; Dave, R. An Analysis of IoT Cyber Security Driven by Machine Learning. In Proceedings of the International Conference on Communication and Computational Technologies: ICCCT 2021; Springer: Singapore, 2021; pp. 725–753.

[15] Andrade, R.O.; Yoo, S.G.; Tello-Oquendo, L.; Ortiz-Garces, I. A Comprehensive Study of the IoT Cybersecurity in Smart Cities. IEEE Access 2020, 8, 228922–228941.

[16] Strielkina, A.; Illiashenko, O.; Zhydenko, M.; Uzun, D. Cybersecurity of Healthcare IoT-Based Systems: Regulation and Case- Oriented Assessment. In Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, 24–27 May 2018; pp. 67–73.

[17] Kulik, T.; Tran-Jorgensen, P.W.V.; Boudjadar, J.; Schultz, C. A Framework for Threat-Driven Cyber Security Verification of IoT Systems. In Proceedings of the 2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), Västerås, Sweden, 9–13 April 2018; pp. 89–97.

[18] Liao, B.; Ali, Y.; Nazir, S.; He, L.; Khan, H.U. Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review. IEEE Access 2020, 8, 120331–120350.

[19] Radanliev, P.; De Roure, C.; Cannady, S.; Montalvo, R.M.; Nicolescu, R.; Huth, M. Economic impact of IoT cyber risk-analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance. In Living in the Internet of Things: Cybersecurity of the IoT; Institution of Engineering and Technology: London, UK, 2018.

[20] Li, S.; Bi, F.; Chen, W.; Miao, X.; Liu, J.; Tang, C. An Improved Information Security Risk Assessments Method for Cyber-Physical- Social Computing and Networking. IEEE Access 2018, 6, 10311–10319.

[21] Ryoo, J.; Tjoa, S.; Ryoo, H. An IoT Risk Analysis Approach for Smart Homes (Work-in-Progress). In Proceedings of the 2018 International Conference on Software Security and Assurance (ICSSA), Seoul, Republic of Korea, 26–27 July 2018; pp. 49–52.

[22] Augusto-Gonzalez, J.; Collen, A.; Evangelatos, S.; Anagnostopoulos, M.; Spathoulas, G.; Giannoutakis, K.M.; Votis, K.; Tzovaras, D.; Genge, B.; Gelenbe, E.; et al. From Internet of Threats to Internet of Things: A Cyber Security Architecture for Smart Homes. In Proceedings of the 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Limassol, Cyprus, 11–13 September 2019; pp. 1–6.

[23] Corallo, A., Lazoi, M., & Lezzi, M. Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. Computers in industry 2020, 114, 103165.

[24] Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. IEEE Communications Surveys & Tutorials 2019, 21, no. 3, 2702-2733.

[25] Mullet, V., Sondi, P. and Ramat, E. A review of cybersecurity guidelines for manufacturing factories in industry 4.0. IEEE Access 2021, 9, 23235-23263.

[26] Ali, B.; Awad, A.I. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. Sensors 2018, 18, 817.

[27] Radanliev, P., De Roure, D., Nicolescu, R., & Huth, M. A reference architecture for integrating the Industrial Internet of Things in the Industry 4.0. University of Oxford combined working papers and project reports prepared for the PETRAS National Centre of Excellence and the Cisco Research Centre 2019, 2, 26854.47686.

[28] Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. Computers in Industry 2022, 137, 103614.

[29] Mahor, V., Garg, B., Telang, S., Pachlasiya, K., Chouhan, M., & Rawat, R. Cyber threat phylogeny assessment and vulnerabilities representation at thermal power station. In International Conference on Network Security and Blockchain Technology. Springer Nature Singapore 2021, 28-39.

[30] Echeverría, A.; Cevallos, C.; Ortiz-Garces, I.; Andrade, R.O. Cybersecurity Model Based on Hardening for Secure Internet of Things Implementation. Appl. Sci. 2021, 11, 3260.

[31] González, L.; Ruggia, R. Controlling Compliance of Collaborative Business Processes through an Integration Platform within an E-government Scenario. In HICSS, 2020, 1-10.