Cyber Security standards for the Industrial Internet of Things (IIoT)

Atdhe Buja[11,] Marika Apostolova[1], Artan Luma[1], and Ylber Januzaj[2]

[1]University of South East European, Faculty of Contemporary Sciences and Technologies, Tetovo, N. Macedonia
[2]University "Haxhi Zeka", Faculty of Business, Peja, Kosova

Abstract. Actually the industrial revolution known as Industry 4.0 for Industrial Internet of Things (IIoT) has advanced their technology of sensors and the industry is utilizing massively. The industrial internet of things (IIoT) devices are used in several industry sectors including smart cities, manufacturing etc., for a collection of data in their process operations and providing those in the time when it's needed for machines or decision making. The aim of this research study was focused on a systematic literature review of actual solutions provided, and possibly come up with a model of Cyber Security standards for the industrial internet of things (IIoT). Considering the facts of previous scientific work conducted there is a research gap of providing such a solution for the Cyber Security of IIoT based on the latest cyber-attacks, threats. Emerging technologies including digital twin, automation, digitalization, cyber security, Internet of things, 5G/6G, and artificial intelligence have increased their development and spread across the industry by utilizing those but not only by them but also harmful individuals or organizations. In this work, we focus on providing Cyber Security for IIoT protection. Our latest development in security breaches have experienced events with such advanced cyber-attacks in methods and techniques. Protection of IIoT sensors and industrial infrastructure has become an urgent need for identifying, prevention, prediction and response of cyber threats and implementing the right security controls. Cyber Security for the IIoT still is a challenge for the industry, and since there is a research gap we see it as an opportunity to design a model where it can advance the Cyber Security level of IIoT and industrial infrastructure.

Keywords: cyber security model, industrial iot, Internet of things, digital twin, threats, countermeasure

[1] Atdhe Buja: ab29762@seeu.edu.mk

1 Introduction

The IIoT have advanced and their applicability has been increased within the industry [1] and the industrial revolution known as Industry 4.0 has boosted up this trend. IIoT devices have been utilized across all industrial sectors including manufacturing, smart cities, oil and gas refineries. Moreover, with all those emerging technologies by mention one of them Digital twins, the IIoT has become more powerful in the functionality aspects and their capability to be used in different sectors of industry is shifting, changing how digital and physical environments are integrated and operated. The IIoT devices have been considered as a subcategory of the Internet of Things (IoT), they have capability to collect data of automated devices or robots and send them to the information system (IS) [2].

2 Problem definition and background

The cyber physical systems (CPS) are going under a fundamental transformation by utilizing big data and analytics. Industry 4.0 and its emerging technologies like Digital twin within the industry and IIoT is shifting the physical world to a digital one. Thus, advancing technologies are also coming with new threats, especially cyber threats. The utilization of those technologies from harmful individuals or organizations is a serious risk to the industrial infrastructure and IIoT because lately a variety of cyber-attack has occurred with advanced methods and techniques.

The pandemic Covid-19 times have increased the threats and cyber-attacks by targeting mostly the industrial infrastructure including supply-chain, travel, e-commerce etc. and causing security breach and other losses [3, 4]. Moreover, the traditional security has failed in the most recent cyber-attacks cases to protect the industrial infrastructure and IIoT. Cyber Security for the IIoT still is a challenge for the industry to protect from such threats and cyber-attacks. IIoT sensors are being used to collect, transmit data by the industrial sectors within it including most of the critical infrastructure [5].

The focus of the study and continuing research is to design a model where it can advance the Cyber Security level of IIoT and industrial infrastructure.

3 Methodology and preliminary results

The research work is conducted using the methods of a systematic literature review (SLR) which has been selected to collect, analysis the literature for Cyber Security counter measurements on IIoT and industrial infrastructure. Moreover, my future work plan is to conduct further experimentation testing in the lab by following a specified use case scenario of Industry 4.0.

The sources of research work are found by using Internet searching focusing the most relevant research papers from databases including IEEE Xplore, Springer, DL ACM, Web of Science, Scopus and Elsevier. The research question remains to design a model of Cyber Security standards for the IIoT in order to prevent any cyber-attack situation.

The results of the SLR research work [1] confirm the research gap that there is a need for the model of Cyber Security standards for the IIoT which can be utilized in the industrial environment. In several periods of time, a common approach of traditional penetration testing is utilized with the same methods and techniques towards IIoT, web application, information systems etc. [6] [7].

Therefore, continued research on this topic and problem produced a very early model proposal dedicated to the IIoT and industrial infrastructure. The research work on this is ongoing future work and a series of experimentation testing are planned to be conducted, and generate results. The design model of Cyber Security standards for the IIoT offers a counter

measurement for threats and cyber-attacks. To prove such, a model will be gone through a series of experimentation testing by two scenarios with and without the model.
In general, the main line functions of the proposed model of Cyber Security standards for IIoT could integrate the following:

1) Phase one, commonly penetration testing process well known and proper to methodologies including OWASP [8] by utilizing also the resources of CVE and Exploit. Generating the finding results and stored for the following phase two.
2) Phase two, data filtering and sorting operation towards the preparation of a report of findings.
3) Phase three, make a difference with what we have actual solutions, impact level sorting is going to be done based on the vulnerability's categories including high, medium, and low. Moreover, this phase considers the references [9, 10, 11, 12, 13, 14, 15, 16, 17, 18] where later on this paper is explained as a main base for the model. This phase generates a process where it is possible to have recommendations of Cyber Security counter measurements based on phase one, and two findings.
4) Phase four, a component of cost benefit analysis (CBA) will be conducted on the recommendations of phase three and a final checklist report will be generated by considering the most valuable solution for protection based on CBA and given to the organization to consider for further steps of implementation.

Therefore, the below were the description of the main proposed workflow which presents the model of Cyber Security standards for IIoT and industrial infrastructure. This model can be applied in the industry for IIoT to protect from threats, and cyber-attacks.

The most used threat model within the sectors of industries is model of STRIDE, which identifies threats and deep operation technology (OT) and automation, this model can be combined with other models including qTMM, CVSS, and PASTA [19].
Therefore, this proposed model is under way to be designed and finalized but not only also take it over an experiment testing in the lab and compare results for further analysis. This innovative model with integrated Cyber Security for the IIoT and industrial infrastructure will make sure and provide safe communications. As well, a model functions important to the whole workflow of it include Cyber threats, exploits and vulnerabilities which are considered the common industrial attacks [20, 21]. The model, consider and select top common industrial Cyber-attacks [22, 23] include Advanced Persistent Threats (APTs). The phase of the experiment lab for us will verify and confirm the results in output of counter measures. The Table 1 presents the scenario designs for simulation of the model including industry Cyber-attacks by utilizing advanced hacking techniques and methods related to the IIoT and industrial infrastructure.

Table 1 Simulations scenarios in operation for the model

No	Scenario	Laboratory setup
1.	Scenario I	- simulated environment IIoT - virtual infrastructure of servers - offensive security environment - cyber-attacks simulation - not protected with model - external data for cyber-attacks type
2.	Scenario II	- simulated environment IIoT - virtual infrastructure of servers - offensive security environment - cyber-attacks simulation - protected with model - external data for cyber-attacks type

4 Further work and Conclusions

In proposed research the importance of a counter measurement model of Cyber Security standards for the IIoT and industrial infrastructure, its problem and background.
Moreover, we propose this model of Cyber Security standards for the IIoT which can enhance the security of IIoT and industrial infrastructure in protection from threats, and cyber-attacks.

As further work is planned for an environment to be built and experiment testing labs in various scenarios of the selected use case for example smart cities application.

Up to this time, the traditional security approach in case of Cyber-attacks within the industrial infrastructure has not shown proper protection for the time and technological development which has impact on advancing Cyber-attacks in methods and techniques. We will continue our research work to provide solutions for the industrial community for their protection in the Cyber Security world.

5 References

[1] A. Buja, M. Apostolova, A. Luma and Y. Januzaj, "Cyber Security Standards for the Industrial Internet of Things (IIoT)– A Systematic Review," *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA),* no. DOI: 10.1109/HORA55278.2022.9799870, 2022.

[2] S. Munirathinam, "Chapter Six - Industry 4.0: Industrial Internet of Things (IIOT)," *Advances in Computers,* vol. 117, no. 1, 2020.

[3] C. N. Deloitte, "Impact of COVID-19 on Cybersecurity".

[4] Gartner, "7 Security Areas to Focus on During COVID-19," 2020.

[5] R. C. R. H. J. H. N. M. M. M. A. R. A. R. A. M. R. K. S. Mario Ayala, "Industrial Internet of Things (IIOT): Opportunities, Risks, Mitigation," 2019.

[6] S. K. S. K. J. S. J. O. K.-h. L. Ji Woong Jang, "Cybersecurity Framework for IIoT-Based Power System Connected to Microgrid," *KSII Transactions on Internet and Information Systems,* vol. 14, no. 5, 2020.

[7] E. M. S. S. M. P. H. C. Ryan Williams, "Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach," *IEEE International Conference on Intelligence and Security Informatics (ISI),* 2017.

[8] OWASP. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Attack_Surface_Analysis_Cheat_Sheet.html.

[9] NIST, "CYBERSECURITY FRAMEWORK," [Online]. Available: https://www.nist.gov/cyberframework.

[10] NIST, "Guide to Industrial Control Systems (ICS) Security," [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final.

[11] NIST, "Guide to Operational Technology (OT) Security," [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft.

[12] NIST, "Integrating Cybersecurity and Enterprise Risk Management (ERM)," 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286-draft2.pdf.

[13] NIST, "NIST SP 800-53 Rev. 5," [Online]. Available: https://csrc.nist.gov/glossary/term/threat_modeling.

[14] CISA, "Cybersecurity Framework," [Online]. Available: https://www.cisa.gov/uscert/resources/cybersecurity-framework.

[15] CISA, "USING THE CYBERSECURITY FRAMEWORK," [Online]. Available: https://www.cisa.gov/using-cybersecurity-framework.

[16] IEC, "Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models," [Online]. Available: https://webstore.iec.ch/publication/7029.

[17] IEC, "Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program," [Online]. Available: Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models.

[18] IEC, "Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers," [Online]. Available: https://webstore.iec.ch/publication/61335.

[19] FIRST, "Threat Modelling," [Online]. Available: https://www.first.org/global/sigs/cti/curriculum/threat-modelling.

[20] E. DB. [Online]. Available: https://www.exploit-db.com/.

[21] MITRE, "CVE DB," [Online]. Available: https://cve.mitre.org/.

[22] C. I. a. P. S. O. Advanced Persistent Threat Compromise of Government Agencies, "CISA," [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/aa20-352a.

[23] U. Government, "CISA," [Online]. Available: https://www.cisa.gov/uscert/.

[24] IEC, "Understanding IEC 62443," [Online]. Available: https://webstore.iec.ch/searchform&q=62443.

[25] J. Nordine, "OSINT Framework," [Online]. Available: https://osintframework.com/.

[26] FIRST, "FIRST Standards," [Online]. Available: https://www.first.org/standards/.

[27] ENISA, "ENISA Good practices for IoT and Smart Infrastructures Tool," [Online]. Available: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/results#IoT.

Ph.D.(c) Atdhe Buja obtained his MSc degree from University AAB in Computer Science. Atdhe Buja is certified as CEH, MCITP, and OCA. Participated in many advanced trainings in USA, Slovenia, Netherlands, Czech Republic, Japan, Mexico, Albania, Montenegro, North Macedonia, and South Korea; on databases, project planning and management, security, large incidents of cyber security exercises, leadership, ICT strategies, IT Governance knows well frameworks as COBIT, TOGAF, ITIL, Azure AppInsight, Azure SQL. Many of his videos and articles can be found at www.atdheb.com

Assoc. Prof. Dr. Marika Apostolova Docent at South East European University. Link of resume https://www.seeu.edu.mk/en/~m.apostolova

Prof. Dr. Artan Luma full Professor at South East European University (SEEU). Link of resume https://www.seeu.edu.mk/en/~a.luma

Dr. sc. Ylber Januzaj link of resume https://www.umib.net/wp-content/uploads/2020/03/CV_Ylber_Januzaj_English.pdf