A Managerial Review and Guidelines for Industry 4.0 Factories on Cybersecurity

Najam Ul Zia, Ladislav Burita, Aydan Huseynova and Victor Kwarteng Owusu
Tomas Bata University in Zlin, Czech Republic
zia@utb.cz
burita@utb.cz
husenova@utb.cz
owusu@utb.cz

Abstract: The Fourth Industrial Revolution (Industry 4.0) has created a rebellion in traditional factories by introducing the Internet of Things (IoT) and Cyber-Physical Systems (CPS). This revolution has caused increased automation and customized production, which has occurred through a synergy between customer demands, stocks, and supply chains. This synergy has also exposed factories to potential cyber-attack threats. Although there is extensive literature available on the topic of cyber security, however, business owners still assume cyber security as business preservation. This study sheds light on a step-by-step cyber security aspect of manufacturing factories with Industry 4.0. The study presented possible vulnerabilities and threats to the networks and devices used in a factory by dividing them into various common parameters. We reviewed the proposed literature and provided solutions to Industry 4.0 factories regarding cybersecurity challenges. The reviewed articles are divided into four segments, starting from the purpose of the proposal, the adopted methodology, the proposed cyber security solution, and finally the author's evaluation. The study reports on a state-of-the-art cyber security solution for Industry 4.0 factories. The characterization of cybersecurity is also proposed concerning management aspects, by showing that every level of organization has its role. The study also highlighted that cybersecurity could play a crucial role in the creation of value for businesses. It is suggested that despite adding an expert system paradigm for cyber security solutions, factories should also adopt new innovative ways, such as machine learning, digital twins, and honeypots. This review highlights that cyber security is not only a technical concern, but it also needs support from multiple actors of the organization to add it to the comprehensive strategy of an Industry 4.0 factory, and every user must be trained and aware of the cybersecurity risks.

Keywords: industry 4.0, cyber security, cyber solution, internet of things

1. Introduction

In an industry 4.0 environment, the cyber-physical system plays a crucial role in performing decentralized decisions to maximize the customized production capacity of smart factories (Kannengiesser and Müller, 2018). To achieve this important task, the logical systems in an internet of things (IoT) interact and collaborate in real-time to apply all kinds of operational processes, organizational services, and intelligent production solutions(Banafa, 2018). IoTs interconnects sensor, devices and instruments which combine with industrial applications like energy and production management to automate the process at a higher level (Banafa, 2018). This IoTs connection moves on to collect data, exchange it and analyse to facilitate the production performance in the production chain of a factory. It also facilitates the manufacturing section to innovate and produce those parts that looked impossible previously. To fully transform the supply chain to a fully IoT based supply chain, there should be an uninterrupted exchange of information from every step of the production scale. Therefore, for a fully automated system, IoT systems are combined with a multilevel architect, hardware level, network level and upper layers. The hardware-level comprises physical systems like sensors, control systems, actuators, and security mechanisms etc. The network-level consists of physical networking like a combination of wired and wireless networking. Finally, the upper layers collect and transmit data and information from this communication network (Tsiknas *et al.*, 2021). This continuous boost of communication in an Industry 4.0 factory creates a strong need for industrial systems protection from cyber-attacks (Juárez, 2019). All the industrial systems that control the process of production, have continuous access to the internet, and these devices are known as industrial control systems (ICS)(Kargl *et al.*, 2014). SCADA (supervisory control and data acquisition) is known to be the most common type of ICS which are used to collect measurement and support process information (Falco, Caldera and Shrobe, 2018). All these systems are interconnected to IoTs that facilitate the remote monitoring and management of processes. Due to this network and connectivity, the operational efficiency of the production system improves, but at the same time, it poses major challenges to secure this infrastructure regarding integrity, confidentiality, and availability (Falco, Caldera and Shrobe, 2018). Another important point is that all the machines and devices are prepared with an objective to enhance smooth production, but not in a mind to secure the devices, which further deteriorates the integrity of system networks

(Tsiknas *et al.*, 2021). This exploitation of machines and devices to external cyber threats means a compromise that may result in malfunctioning or destruction of the whole production system (Panchal, Khadse and Mahalle, 2018). The current literature focuses on security risks in IoT based factories, however, there is a paucity of literature on the knowledge and clear understanding of threats associated with IoT systems. In this aspect, our study highlights the ways of industrial application attacks and the available solutions in the literature. The paper contributes by providing literature for researchers and for organizations dealing with IoTs technologies on cyber threat issues and also the solutions for protecting these industrial applications and instruments.

The study organizes as follows, section 2 provides a detailed explanation of main industrial IoT environment tasks and the possible effective solutions that are taken out from the available literature. Section 3 shows the results of the study, and then the last section comes with a conclusion and future research possibilities.

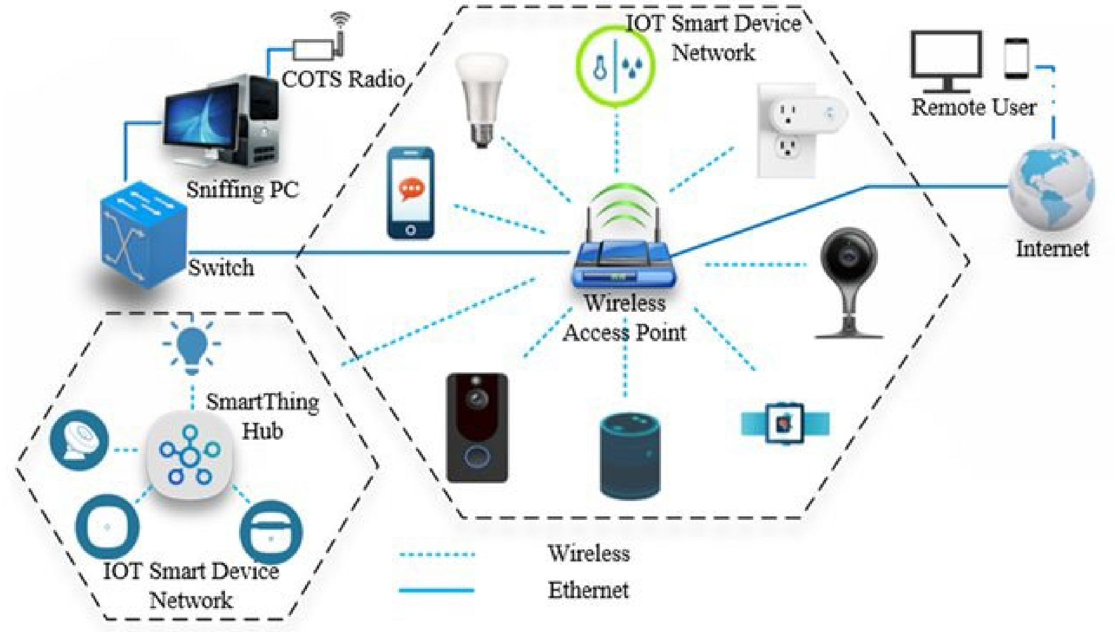

Figure 1: Internet of Things layers (Calix *et al.*, 2020)

2. Cyber threats and possible solutions

To achieve customized production and quality milestones, automation and remote control are considered as most crucial methods in an Industry 4.0 factory (Mikhalevich and Trapeznikov, 2019). This system requires efficient management of IoT systems consisting of maximum accuracy, security, and reliability. The digital infrastructure that is part of these IoT systems improves the critical infrastructure efficiency but meanwhile requires securing the infrastructure against possible cyber-attacks. Not only this brings a need to protect the local digital infrastructure, but it also directs to protect the general crucial digital infrastructure of the country. In the below sections, we have categorized the IoT threats into phishing attacks and supply chain attacks. This categorization presents a clear comprehensive and clear information about cyber risks and the solutions of protection in an Industry 4.0 environment.

2.1 Phishing attacks

This is a typical method of stealing sensitive information from consumers. It occurs when a hacker impersonates a trustworthy entity (Roman *et al.*, 2009) and dupes individuals into entering personal information on a fake website or downloading an attachment, resulting in the installation of malware or the disclosure of sensitive information. Advanced social engineering tactics known as compromised attacks are used by specialized phishers to target important infrastructures. They target both the absence of specific active security measures by systems and the lack of information or attention of users. Generally, a cyber attacker tries to approach the IoT systems through the front end level. Several papers have highlighted the website crawling based techniques. A new technique called PHONEY is proposed by Chandrasekaran, Chinchani and Upadhyaya, (2006) that can automatically detect and highlight phishing attacks. This technique keeps the main idea of a web browser extension, which gives information on website security certificates, quality of websites or a misleading URL.

Another technique is introduced by McRae and Vaughn (McRae and Vaughn, 2007) detects phishing contents sites by using honey tokens. A more promising technique referred to as URL embedding was proposed by Yan *et al.* (2020). They used an algorithm to investigate the correlation between various domain names for a calculation of the correlation coefficient between various URLs.

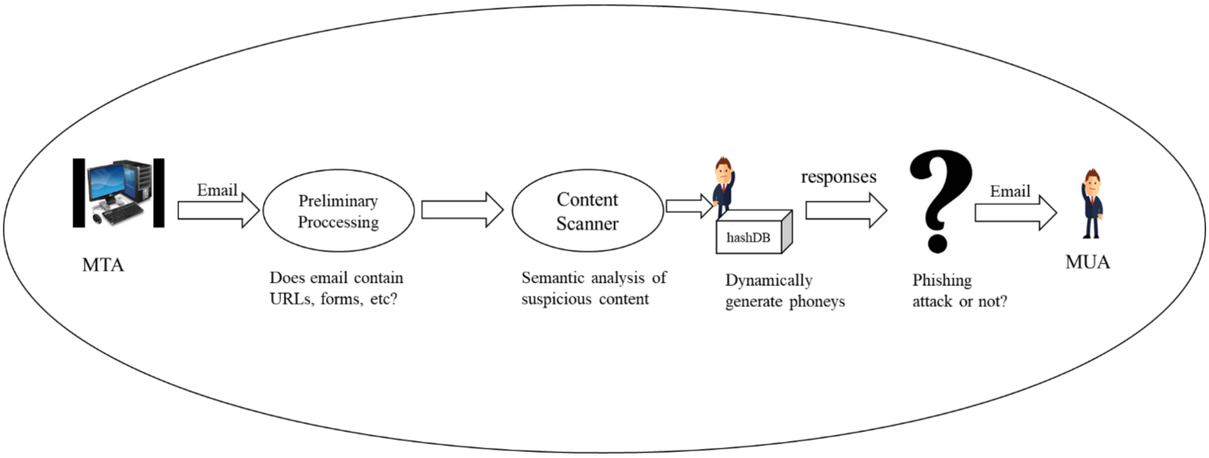
MTA
Email
Preliminary Proccessing
Does email contain URLs, forms, etc?
Content Scanner
Semantic analysis of suspicious content
hashDB
Dynamically generate phoneys
responses
Phishing attack or not?
Email
MUA

Figure 2: PHONEY architecture

2.2 Supply chain attacks

Supply chain attacks are considered as most dangerous. Security is the major challenge in the supply chain of Industry 4.0. It is difficult to find the hardware chips with implanted malicious code because this code can be executed for a long time without being noticed. Another cause of security weaknesses is the stakeholders' involvement. The device acquisition system is not unique and centralized. Because different kinds of devices are manufactured by different vendors, then assembled by another vendor and at the end distributed by a different vendor. Due to this situation, many security issues arise. Therefore, risk management is getting more and more attention day by day.

A study by Farooq and Zhu, 2019; Kieras, Farooq and Zhu (2020, sheds the light on supply chain threats and suggest various approaches concerned with risk management methods. The study highlighted the risks involved to IoT supply and define it as extremely diverse. Though the study has a general understanding of the risks of the supply chain, however, it did not provide the possible solutions or countermeasures to address these kinds of attacks in an Industry 4.0 environment. In a study by Radanliev *et al.* (2020), a self-adapting and dynamic supply chain system is introduced which is supported by real-time intelligence, machine learning (ML), and artificial intelligence (AI). This approach is castoff for small and medium enterprises (SMEs) to grow a transformational roadmap for the Industry 4.0 Industrial Internet of Things, as small companies lack resources to mitigate the high cyber-attack risks. The cyber risk measurement is due to the weakness of understanding Industry 4.0 supply chain operations. Kieras, Farooq and Zhu (2020) stated in their study about the risk analysis of IoT supply chain threats. They introduced an adoption of attack free technique associated with vendors and suppliers. They intend to highlight and uncover the threats that are associated with potential supplier collusion

A vendor can incorporate backdoor routes in their equipment, implant viruses, or supply defective chips. The hazards in the supply chain are difficult to detect and control. As the IoT ecosystem becomes more complicated, the risk spreads from one device to the next. Another challenge is dissecting the supply chain linkages in IoT, which means that determining the relationships between devices, suppliers, and among them is always challenging. They also underline the implications and repercussions of IoT hazards, and as a protective measure, they recommend seeing the ecosystem from a supply chain perspective and then taking appropriate risk-control measures. They distinguish between two approaches: the top-down method, which is more centralized, and the bottom-up approach, which emphasizes decentralization. This study provides a broad knowledge of supply chain risks, but it does not include technological remedies for dealing with these sorts of attacks in a context that is already facing this danger and cannot adapt 's entire risk management system. In this paper, Radanliev *et al.* (2020), propose a dynamic and self-adapting supply chain system powered by artificial intelligence (AI), machine learning (ML), and basic intelligence for predicted cyber risk analytics. This method is used to create a transformative roadmap for the Industrial Internet of Things in Industry 4.0 supply chains of small and medium businesses (SMEs) because these organizations typically lack the resources required to successfully combat the significant risks posed by cyber-attacks. The inability of existing cyber risk impact assessment methods to measure the impact of supply chain infrastructure is an intriguing topic of debate from the major findings. Furthermore, due to a lack of understanding of supply chain activities in Industry 4.0, there is inconsistency in quantifying supply chain cyber threats. Kieras, Farooq and Zhu (2020) in this study introduced the RIoTS (risk analysis of IoT supply chain threats) technique in their paper, which is risk analysis methodology in network infrastructures such as the IoT that arise from single components providers. They believe that risk analysis should move away from a vulnerability-centred strategy and toward modelling suppliers and elements as a system. They suggest modifying attack tree methodologies to account for the risk associated with suppliers and supplier groupings. Their goal is to expose and uncover hidden dangers to the IoT ecosystem caused by potential supplier collaboration. As we've seen, the majority of research concentrate on risk management measures for supply chain assaults.

3. Discussion

The general security of the infrastructure and the dependability of the intended solutions stated should not be taken for granted, since the cyber security of the IoT ecosystem is a multifactorial dilemma (Nakamura and Ribeiro, 2018). Particularly, due to the landscape of the IoT and the extensive series of exposures that can happen from the intricacy of the systems tangled in it, significant structures related to multifaceted patterns, systems, or procedures are recognized and preserved, which do not develop in parallel with the overtime and which are possible weaknesses of the entire network (Sengupta, Ruj and Bit, 2020). More commonly, the problem deceits in the fact that in the specific high intricacy atmosphere under inspection, while adjustment systems are multivariate, high assortment happens and is preserved, as this can be accredited to the age of systems that have not been promoted, to the composite connection that defines them, and the delicate alterations that differentiate them (Lee and Chen, 2019).

Among the threats stated, the supply chain incidents are turning out to be a severe concern, because substantial issues like complexity and stealth do not offer simple solutions. To diminish these types of attacks, typically risk management methods are utilized. Another main disadvantage is the fact that older industrial systems, which in most cases do not have security as a precondition in their structure stipulations, are spinning points of the complete security of the system, suggestively growing the overall hazard of attacks, even if access control or encoding methods are added in them (McLaughlin *et al.*, 2016). In addition, the adjustment and organizing events with the existing established standards raise thoughtful alarms, as most of the current IoT systems have an extraordinary degree of dependency on their development company, which generates difficulties of reorganization or revision of their mechanisms, such as functions that they contain or can support (Lee and Chen, 2019). Moreover, due to the real-time process and progress of the IoT, the supervision of data with the time difference, taking into account correlations from other instruments or devices that may be incorporated in the data flow categorization, creates additional requirements in the ways of confirming accuracy and integrity of information. While offering tight requirements, the encrypt (Nakamura and Ribeiro, 2018) and key management approaches suggested and utilized in the IIoT environment fall behind in the development of mechanisms that will be implemented fast and without much complexity, allowing them to be employed by low-resource devices. Subsequently, a further important finding through the use of most of the machine learning techniques presented in the literature is that only statistics on the system or network traffic are used (Zhou and Guo, 2018), resulting in ineffective smoothing because the metrics trained do not include a variety of aspects from different uses or behavioural parameters of the system overall. The error originates from the mistaken assumption that the initial version and all of its updated duplicates had identical features distributions, and so the current statistics could be shared with all of the intelligent learning inner current adjustments. Another better approach, which was used in the suggested method, is to save statistics throughout stages and read the optimizing parameters methodically to every inner loop iteration.

4. Conclusion

Given the increasing complexity of threats in the ever-changing environment of the Industrial IoT, as well as the parallel vulnerability of existing security systems to detect significant threats of increasing magnitude and duration, it is necessary to recognize the risks that threaten particular infrastructure and services and provide industrial data confidentiality (McLaughlin *et al.*, 2016). Likewise, while there is a chance that hackers may get access to the manufacturing process, perhaps with disastrous, if not incalculable, effects, most industrial organizations seek security know-how to defend their infrastructure. It should have been highlighted that IoT designs and industrial systems in general (Kargl *et al.*, 2014; Falco, Caldera and Shrobe, 2018) require a separate type of protection than regular networks, because traditional security solutions, such as virus scanners and traditional firewalls, do not match industry norms and criteria. A thorough description of attacks against Industrial IoT systems was carried out in this study, considering the most important features and vulnerabilities that they incorporate, as well as a thorough analysis of indicative solutions against these vulnerabilities, as proposed in the most recent literature. It is a proven reference framework and an indicative scientific presupposition in this context for the identification and evaluation of hazards associated with the ever-changing industrial environment. One factor that might be addressed in the future extension of this research is the analysis of unconventional ways of attack or innovative techniques of combined approach of unknown assaults such as zero-day attacks. Lastly, the research might be broadened by looking into unique protective strategies against IoT, the physical security of IoT devices, from malicious setup of mechatronic subsystems that are part of this network, with the goal of exploitation by a third – party for example vendors.

References

Banafa, A. (2018) '2 the industrial internet of things (IIoT): challenges, requirements and benefits'.

Calix, R. A. *et al.* (2020) 'Cyber Security Tool Kit (CyberSecTK): A Python Library for Machine Learning and Cyber Security', *Information*, 11(2), p. 100.

Chandrasekaran, M., Chinchani, R. and Upadhyaya, S. (2006) 'Phoney: Mimicking user response to detect phishing attacks', in *2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06)*. IEEE, pp. 5-pp.

Falco, G., Caldera, C. and Shrobe, H. (2018) 'IIoT cybersecurity risk modeling for SCADA systems', *IEEE Internet of Things Journal*, 5(6), pp. 4486–4495.

Farooq, M. J. and Zhu, Q. (2019) 'IoT supply chain security: Overview, challenges, and the road ahead', *arXiv preprint arXiv:1908.07828*.

Juárez, F. A. B. (2019) 'Cybersecurity in an Industrial Internet of Things Environment (IIoT) challenges for standards systems and evaluation models', in *2019 8th International Conference On Software Process Improvement (CIMPS)*. IEEE, pp. 1–6.

Kannengiesser, U. and Müller, H. (2018) 'Towards viewpoint-oriented engineering for Industry 4.0: A standards-based approach', in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. IEEE, pp. 51–56.

Kargl, F. *et al.* (2014) 'Insights on the security and dependability of industrial control systems', *IEEE security & privacy*, 12(6), pp. 75–78.

Kieras, T., Farooq, M. J. and Zhu, Q. (2020) 'RIoTS: Risk analysis of IoT supply chain threats', in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*. IEEE, pp. 1–6.

Lee, J.-C. and Chen, C.-Y. (2019) 'Exploring the determinants of software process improvement success: A dynamic capability view', *Information Development*, 35(1), pp. 6–20.

McLaughlin, S. *et al.* (2016) 'The cybersecurity landscape in industrial control systems', *Proceedings of the IEEE*, 104(5), pp. 1039–1057.

McRae, C. M. and Vaughn, R. B. (2007) 'Phighting the phisher: Using web bugs and honeytokens to investigate the source of phishing attacks', in *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*. IEEE, pp. 270c-270c.

Mikhalevich, I. F. and Trapeznikov, V. A. (2019) 'Critical infrastructure security: Alignment of views', in *2019 Systems of Signals Generating and Processing in the Field of on Board Communications*. IEEE, pp. 1–5.

Nakamura, E. T. and Ribeiro, S. L. (2018) 'A privacy, security, safety, resilience and reliability focused risk assessment methodology for IIoT systems steps to build and use secure IIoT systems', in *2018 Global Internet of Things Summit (GIoTS)*. IEEE, pp. 1–6.

Panchal, A. C., Khadse, V. M. and Mahalle, P. N. (2018) 'Security issues in IIoT: A comprehensive survey of attacks on IIoT and its countermeasures', in *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*. IEEE, pp. 124–130.

Radanliev, P. *et al.* (2020) 'Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains', *Cybersecurity*, 3, pp. 1–21.

Roman, R. *et al.* (2009) 'Trust and reputation systems for wireless sensor networks', *Security and Privacy in Mobile and Wireless Networking*.

Sengupta, J., Ruj, S. and Bit, S. Das (2020) 'A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT', *Journal of Network and Computer Applications*, 149, p. 102481.

Tsiknas, K. *et al.* (2021) 'Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures', *IoT*, 2(1), pp. 163–186. doi: 10.3390/iot2010009.

Yan, X. *et al.* (2020) 'Learning URL embedding for malicious website detection', *IEEE Transactions on Industrial Informatics*, 16(10), pp. 6673–6681.

Zhou, L. and Guo, H. (2018) 'Anomaly detection methods for IIoT networks', in *2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*. IEEE, pp. 214–219.