A review Cyber of Industry 4.0 (Cyber-Physical Systems (CPS), the Internet of Things (IoT) and the Internet of Services (IoS)): Components, and Security Challenges.

Husham I. AL-Salman *1, Muataz H. Salih 1,2

1School of Computer Engineering, Universiti Malaysia Perlis, 01000 Kangar, Perlis, Malaysia.
2IR4.0 and Intelligent Automation Group, Core Engineering, Plant 5, Flex. 13600 Prai, Penang, Malaysia.

*Correspondence Author: husham.alsalman90@gmail.com

Abstract. The term Industry 4.0 as well as Cyber Physical System has lately gained a lot of consideration among most of the researchers as well as manufacturers while bringing in possible improvement solutions for maintenance of advanced technologies. The term Cyber Physical System or CPS is defined as the addition of computational and physical procedures on the technology of Internet of Things. This prototype helps in ensuring the connectivity of devices and elements with the Internet based protocols which includes the Internet of Services. This pattern of connectivity also enables horizontal services of internal factory through the entire value chain. However, there are several challenges that are faced while maintain the theories and practices of the above protocols. This part of the paper aims at providing a better understanding of the challenges that are faced by these components. The challenges that are faced by CPS are hence described with the help of further researches and are thus summarized from the perspective of energy control, transmission, secure control as well as management control techniques including allocation of system resources and designing of software based models. The paper also reflects the challenges that are faced by IoT from the perspective of communication security, protection of data through sensors and algorithms based on cryptography. Finally the paper also describes the challenges of IoS that are developed through cloud aggregation technology, allowing cloud providers to interact and collaborate in the improvement of cloud security infrastructure including its energy efficiency and reliability.

1. Introduction

This theory comparatively investigates about the smart factories that are controlled with the help of Cyber Physical Systems that executes the simple and iterative activities that were previously carried out by humans. Here the execution process is presumed to be relied on awareness based on machines and their auto agonistics and auto configurations [1]. Here everything is supported by the interconnection of machines and their components via computer based methods. The products and the machines are well equipped with the microchips that help in facilitating the processes while customizing the operations over the Internet and cloud loading while utilizing the data centers, 3D printing services and automated problems related to smart warehouses on a regular basis. The tools and techniques that are used with the Industry 4.0, are considered to save a lot of stretch as well as
costs while improving the flexibility of businesses and manufactures on a basis of large scale including all the major type of risks like hacking of computer systems and misusing the data [2]. The Industry 4.0 could potentially improve the quality of living while increasing the amount of productivity from the workforce and eliminating the monotonous culture of work which includes demanding of jobs physically. The term Industry 4.0 is usually used to denote the current position of digitization that are related to automated process of manufacturing. At ye Hannover Fair held in the year 2013, the concept of Industry 4.0 was first introduced [3]. With this the concept led to the opening of a diverse range of opportunities while putting systems within their specified positions considering all the types of threats that are simultaneously published through data based on industrial system attacks indicating a worst situation with occurrence of more number of attacks directed at the control systems. The Internet Security threat report as published by the Symantec confirmed the fact that “attackers are more likely to choose systems that can be easily compromised and suggests evidence that SCI is particularly vulnerable”. The entire section based on this confirmation is published in its report based on Threats Predictions which is issued annually describing the major threats faced by industries. The threats of Cyber-attacks manipulating the workflow system and processes are escalated through the challenges that are faced by the Industrial Internet [3]. This can lead to disruption or outages causing enormous costs. Recently, a survey was conducted by Deloitte shows that the manufacturers believe for the potential rise in the cyber risks as a result of the transformation to Industrial 4.0. For example, as per the report published by the Department of Homeland Security of U.S the cyber-attacks on manufacturing sectors are going to rise at a double rate within one year. This gradual increase in security incidents will cause a great cost leading to financial loss and compromising the security to about 38% than the past years [4].

2. Cyber Challenges in Industry 4.0

The Cyber security in the era of Industry 4.0 has a direct outcome on the Cyber Physical Systems, Internet of Services as well as on the Internet of Things [5].

2.1. Cyber Physical Systems (CPS)

A cyber physical system is a type of scheme that monitors the physical systems while creating a virtual copy and developing decisions in a decentralized way[6]. Within the Cyber physical system, the control elements and the sensors of the system are connected with machines and devices along with installations, networks, vessels and human beings.
The system refers to the new group of systems which have combined physical and computational capabilities enabling interaction through various new modalities [18]. System and Control researchers have pioneered themselves in various researches conducted over years on the development of science of powerful systems and engineering techniques such as domain methods of frequency and time, analysis of state-space, identification of systems, prediction, controlling robustness, filtering and controlling stochastic [12]. Researchers have also made further studies based on the new type of programming languages, methods of visualizations, techniques for real time computing, compiler designing architectures of embedded systems, software systems as well as various innovative techniques to ensure the reliability of computer systems, their security and fault tolerance capability. Researches have also tried developing varieties of modeling and powerful verification tools. All these challenges mentioned above are now being studied so as to find solution using the modern FPGA technology.

2.2. Internet of Things (IoT).

The Internet of Things is acted upon by the CPS. This protocol helps in ensuring that the strategies and elements are well linked to the Internet based Protocols or the TCP/IP. The challenges that are being reached under the IoT are represented below:

| NO | SECURITY CHALLENGE                     | RF |
|----|----------------------------------------|----|
| 1  | Laws and Regulations regarding security: The laws and regulations of security are still [19] not in place and also there is no such standard technologies related to IoT. IoT is mainly related to the security of national information including business secrets and personal privacy. |    |
2 Key Management: Key management is one of the basic mechanisms of security and is mostly researched. It is regarded as the most critical aspect of security of cryptography. Still no such solutions have been identified by researchers about its security and the algorithms of cryptography based on high performance sensors are still not applied in many cases. In this case the real networks of large scale sensors are put into practices.

3 Domain Name System: The main challenge that arises during identification of object is to determine the integrity of the records that are used during naming of architectures. Although the DNS helps in providing translation to the names of services to the Internet users, it is regarded as an unsecured way of naming system as it is vulnerable to various cyber-attacks such as poisoning attack of DNS Cache or man in the middle attack.

4 Burgeoning Application requirements: With the introduction of RFID, WSNs, technology related to network communication, various computing technologies and various control theory for real time distribution, the CPS is regarded as an emerging form of IoT technology with high risk of security over its system performance.

5 Privacy and trusts: With the use of monitoring and remote sensors in the IoT Technology, the controlling access along with the ownership of data are becoming highly sensitive.

6 Absence of Global root CA has become one of the challenges for authentication system, causing infeasibility in certifying objects related to IoT. Hence this needs to be taken into consideration as it will also lead the high computational methods to suffer.

7 High cost security against malware: While shifting from the x86 architecture, the conventional methods of security can be infeasible against malware leading to issues such as divergence of the architecture of hardware among various strategies. Without the proper malware abstraction of IoT, the current solutions related to ad-hoc remains inapplicable.

8 Crypto-systems: In spite of having advantages of the public key cryptosystem, there remains a lack of root certificate authority over authentication of construction schemes that are actually deployed.

Since the past few decades, the Internet of Things has been the main area of researches. Security and privacy has been the main issues for the application of IoT including several other challenges facilitating the domains and reviewing the research progresses of IoT paying special attention to the security. While thoroughly analyzing the security features and architectures of IoT the requirements of security are established. Based on theses researches, the technologies including the mechanism of encryption, security of communication, protection of sensor data and algorithms based on cryptography are hence outlined through the challenges.

2.3. Internet of Services (IoS):

The IoS protocol offers a variety of services of internal factory running horizontally throughout the value chain [29]. The challenges that are being reached under the IoS are represented below:

| NO | SECURITY CHALLENGE | RF |
|----|-------------------|----|
| 1  | Scalability of services: Although there are many services that are static in nature from the view pint of their size but still the services experiences fluctuations due to workload. | [30] |
| 2  | Monitoring of Services: Most of the mechanism of billing including payment as offered by providers are based on resources of individual users as per their consumption time based on unit. | |
| 3  | Context awareness of applications: One of the key challenges of the future of IoS is to address the increase in the information relevancy within a given context. Of becoming more aware in specific application and services such as social networking, computational environment and various other mobile applications. This context awareness adapts certain behaviors related to the environment such as activity of users, accessing of devices, location or people who are nearby. | [31] |
Cloud computing plays a vital part in the upcoming of Internet of Services while allowing provision of on-demand requests, computational infrastructures and platforms. The communal part in cloud needs to address the challenges that are faced technically while turning the visions into reality. Some of the issues that make the cloud service providers to collaborate and improve the security, efficiency and reliability of the cloud infrastructures include elastic service platforms, managing of clouds efficiently and delivering of scalable cloud services.

3. References

[1] Sonntag, D., Zillner, S., van der Smagt, P., and Lörincz, A., 2017 Industrial Internet of Things, Springer, pp. 487–504

[2] Zezulka, F., Marcon, P., Vesely, I., and Sajdl, O., 2016 IFAC-PapersOnLine, 49(25), pp. 8–12

[3] Marcon, P., Zezulka, F., Vesely, I., Szabo, Z., Roubal, Z., Sajdl, O., Gescheidtova, E., and Dohnal, P., 2017 Prog. Electromagn. Res. Symp., Part F1343, pp. 1694–1697

[4] Symantec, 2016 SMARTER SECURITY FOR MANUFACTURING IN THE INDUSTRY 4.0 ERA

[5] Dulaunoy, A., Iklody, A., and Vinot, R., 2016 APCO interational, 1.0, p. 24

[6] Brookson, C., 2016 ETSI, (18)

[7] Jirkovský, V., Obitko, M., and Mařík, V., 2017 IEEE Trans. Ind. Informatics, 13(2), pp. 660–667

[8] Rasmussen, T. B., Yang, G., Nielsen, A. H., and Dong, Z., 2017 2017 IEEE Manchester PowerTech, Powertech 2017

[9] Benias, N., and Markopoulos, A. P., 2017 South-East Eur. Des. Autom. Comput. Eng. Comput. Networks Soc. Media Conf. SEEDA-CECNSM 2017

[10] Flatt, H., Schriegel, S., Jasperneite, J., Trsek, H., and Adamczyk, H., 2016 IEEE Int. Conf. Emerg. Technol. Fact. Autom. ETFA, 2016–Novem

[11] Humayed, A., Lin, J., Li, F., and Luo, B., 2017 IEEE Internet Things J., 4662(c), p. 30

[12] Lee, E. A., 2015 Sensors (Switzerland), 15(3), pp. 4837–4869

[13] Taylor, J. M., and Sharif, H. R., 2017 Selected Topics in Mobile and Wireless Networking (MoWNeT), 2017 International Conference On, IEEE, pp. 1–6

[14] Rawat, D. B., White, T., Parwez, M. S., Bajracharya, C., and Song, M., 2017 IEEE Internet Things J., 4(6), pp. 1987–1993

[15] Ali, S., Al Balushi, T., Nadir, Z., and Hussain, O. K., 2018 Cyber Security for Cyber Physical Systems, Springer, pp. 1–10

[16] Jia, Y., Chen, Y., Dong, X., Saxena, P., Mao, J., and Liang, Z., 2015 Comput. Secur., 55, pp. 62–80

[17] Liu, S., Liu, X. P., and El Saddik, A., 2013 Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES, IEEE, pp. 1–6

[18] Habib, H. F., Lashway, C. R., and Mohammed, O. A., 2017 2017 IEEE Ind. Appl. Soc. Annu. Meet. IAS 2017, 2017–Janua, pp. 1–8

[19] Banafa, A., 2015 OpenMind, (March), pp. 16–27

[20] Murphy, M., 2017 Netw. Secur., 2017(7), pp. 17–19

[21] Turmel, V., Anderson, E., and Security, I., 2016 Industrial Security : Applying IoT Security Controls on the Industrial Plant Floor

[22] Ni, J., Zhang, K., Lin, X., and Shen, X., 2017 IEEE Commun. Surv Tutorials

[23] Yogita Pundir, M., Sharma, M. N., and Singh, Y., 2016 Int. J. Adv. Res. Comput. Commun. Eng., 5(3), pp. 960–964

[24] Guan, C., Ren, K., Zhang, F., Kerschbaum, F., and Yu, J., 2015 European Symposium on Research in Computer Security, Springer, pp. 203–223

[25] Herder, C., Fuller, B., van Dijk, M., and Devadas, S., 2017 IACR Cryptol. ePrint Arch., 2017, p. 210

[26] Singh, S., 2015 Int. Conf. Green Comput. Internet Things, pp. 1577–1581
[28] El-Hadedy, M., Skadron, K., Mihajloska, H., and Gligoroski, D., 2015 Proc. Hear.
[29] Moreno-Vozmediano, R., Montero, R. S., and Llorente, I. M., 2013 IEEE Internet Comput., 17(4), pp. 18–25
[30] Liu, L., 2016 IEEE Trans. Serv. Comput., 9(5), pp. 661–663
[31] Yurur, O., Liu, C., and Moreno, W., 2014 IEEE Commun. Mag., 52(6), pp. 24–31