The Emergence of IIoT and its Cyber Security Issues in Critical Information Infrastructure

Humairaa Yacoob Bhaiyat and Siphesihle Philezwini Sithungu
Academy of Computer Science and Software Engineering, Faculty of Science, University of Johannesburg, South Africa
humairaabhaiyat@gmail.com
siphesihles@uj.ac.za

Abstract: The emergence of the Industrial Internet of Things (IIoT) can transform and improve industrial domain processes. This is achieved by IIoT's ability to collect and process vast amounts of data using technology such as sensors. IIoT capabilities can improve the manufacturing processes of these sectors and contribute to the improved functioning of critical information infrastructure. In addition, current trends - such as the Fourth Industrial Revolution (4IR) - use IIoT to realise specific goals. While the emergence of IIoT systems does introduce many benefits, such as improved efficiency and sustainability, it can also introduce security concerns. These security concerns pose a significant threat to the industrial domain, including critical information infrastructures. The resulting threats emphasise the need to implement solutions to secure IIoT systems. The paper aims to discuss the emergence of IIoT and its cyber security issues within the context of critical information infrastructure. The research paper follows a theoretical research methodology to provide an improved understanding of the emergence of IIoT and its cyber security issues in critical information infrastructure. The paper contains an exhaustive discussion of what is IIoT. A discussion on where IIoT fits within the context of critical information infrastructure and its impact on 4IR is also highlighted in the paper. Due to the many vulnerabilities that IIoT systems can contain, the paper also discusses security concerns surrounding the emergence of IIoT. The security concerns make IIoT systems attractive targets for cyberattacks. Therefore, different approaches that can be applied to secure IIoT systems is also provided. Since IIoT capabilities can impact the critical information infrastructure of businesses and nations, the authors' stance on how IIoT systems could transform the current understanding of critical information infrastructure is also discussed.

Keywords: internet of things, industrial internet of things, critical information infrastructure, fourth industrial revolution, security concerns

1. Introduction

The Industrial Internet of Things is an emerging field that can assist in improving the industrial sector by expanding manufacturing, agriculture, and military processes (Jaidka, Sharma & Singh, 2020). The emergence of IIoT systems can also impact both critical information infrastructure (CII) and the 4IR. The role that IIoT plays within CII and the 4IR can benefit these two domains through its ability to collect and process vast amounts of data (Serpanos & Wolf, 2017). However, due to the increased use of IIoT systems, there are security concerns surrounding the emergence of IIoT systems. These security concerns emphasise that security approaches that protect the integrity of IIoT devices must be designed and implemented (Sadeghi, Wachsmann & Waidner, 2015). The abilities and security concerns surrounding IIoT can transform the ability of CIIs to manage and control CI.

This research paper aims to discuss the emergence of the IIoT and its cyber security issues within the context of CII. The paper is structured in the following manner to achieve this objective: Section 2 discusses IIoT. Section 3 provides a discussion on the role IIoT can have on CII. Section 4 highlights the impact that the IIoT can have on the Fourth Industrial Revolution. Section 5 discusses security concerns surrounding the emergence of IIoT. Section 6 discusses different approaches that can help secure IIoT systems. Section 7 discusses the authors' view on how IIoT could transform CII. The last section, Section 8, concludes the paper.

2. What is the industrial internet of things?

The concept of the Internet of Things (IoT) and IIoT are closely related. However, there are differences between them (Sisinni, Saifullah, Han, Jennehag, & Gidlund, 2018). To understand IIoT, one should first understand the difference between IoT and IIoT. The basic concepts between IoT and IIoT are similar: interconnected smart devices that perform data collection, remote sensing, processing, monitoring and control (Serpanos & Wolf, 2017). However, the focus of IoT is human-centered (i.e., smart consumer devices that are interconnected with one another to make people's lives easier in terms of saving time and money) (Sisinni et al., 2018). In comparison, IIoT's focus is safety and operation, which includes the operational technology used in the industrial sector (Serpanos & Wolf, 2017). IIoT combines information and Communication Technology (ICT) trends with industrial

production systems (Arnold, Kiel & Voigt, 2016). IIoT can also be seen as a subset of IoT that operates in the industrial sector (Serpanos & Wolf, 2017). The main goal of IIoT is to integrate industrial control systems, analytics, business processes, and enterprise systems (Bajramovic, Gupta, Guo, Waedt & Bajramovic, 2019).

IIoT can also be described as communication between machines. These machines communicate and interact with other objects and machines (Simon, 2017). This communication can lead to optimal industrial operations because IIoT can detect failures. IIoT systems can activate the manufacturing process, obtain information from different objects and sensors and send readings to the cloud-based centres (Sisinni et al., 2018; Wan, Tang, Shu, Li, Wang, Imran & Vasilakos, 2016). Sensors are key IIoT technologies as they produce different kinds of data, which must be precise and is usually predictive. Other key technologies are Big Data and advanced analytics for predictions, historical analysis, and insight on machines and processes (Gilchrist, 2016). IIoT can also transform businesses by improving worker safety, worker productivity, sustainability, customer experience, reducing operational costs, and creating new revenue streams (Simon, 2017). These capabilities have resulted in the emergence of IIoT in CII. The following section discusses where IIoT fits within CII.

3. Where does Industrial IoT fit within critical information infrastructure?

IIoT can be applied to different areas, but one of the main areas that can benefit from the applications of IIoT is critical infrastructure (Mcginthy & Michaels, 2019). Critical infrastructures are managed and controlled through CIIs. CIIs manage and control other systems that provide essential economic services, such as gas utilities, electrical power grids, air transportation, and many other crucial systems (Lopez, Setola & Wolthusen, 2012). Furthermore, CII systems are controlled by remote systems, also known as Industrial Control Systems (ICS), such as supervisory control and data acquisition (SCADA) systems. Therefore, IIoT can be integrated within CII to improve efficiency in critical areas (Mcginthy & Michaels, 2019).

IIoT can lead to efficient management by intelligently processing and analysing the huge amounts of data obtained from communications between the different machines in critical areas such as transportation, energy, medical, etc. (Simon, 2017). IIoT can do this because wireless sensor networks and IIoT allow for the sensors to be placed in remote locations that provide data to the central system. This can be done across many CII sectors (Mcginthy & Michaels, 2019). However, considering the application of IIoT to CIIs, a failure in IIoT can lead to life-threatening situations (Magomadov, 2020). Examples of IIoT applied in CIIs would be automated vehicles that use sensors to reduce the exposure of noise, hazardous gases, and chemicals to workers involved in industries such as gas and oil (Agenda, 2015).

Nations such as the United Kingdom have started integrating IIoT in their CII. Some providers of wastewater services and drinking water in the United Kingdom use a combination of IIoT sensors, real-time data, and analytics to determine and anticipate equipment failures and respond quickly to emergencies such as water leakage (Simon, 2017). These examples show that IIoT can augment CII to provide automation to optimise operations. The optimisation of IIoT can also impact 4IR. The following section discusses the impact of IIoT on 4IR.

4. Impact of Industrial IoT on the fourth industrial revolution

IoT and IIoT can assist in understanding the impact of the Fourth Industrial Revolution (4IR), also known as Industry 4.0 (Mcginthy & Michaels, 2019). The Fourth Industrial Revolution can be described as digitalising the manufacturing sector by embedding sensors in virtually all cyber-physical systems, manufacturing equipment and product components. 4IR also includes analysing the data generated by sensors for effective decision-making (Lampropoulos, Siakas & Anastasiadis, 2019). For this reason, it is believed that the Fourth Industrial Revolution began with the inception of IIoT (Jaidka, Sharma & Singh, 2020). IIoT achieves key features of 4IR, such as horizontal integration. IIoT achieves horizontal integration through value networks for supporting companies' business strategies. Other key features include vertical integration and integrating the digital with the real world in the value chain, thus achieving end-to-end integration (Pivoto, de Almeida, da Rosa Righi, Rodrigues, Lugli, & Alberti, 2021).

IIoT is also seen as one of the drivers of 4IR. IIoT, automation, and the digitalising of the industrial manufacturing sector are believed to be drivers that initiated 4IR. IIoT in 4IR can also improve and change current industries by improving productivity, reducing costs and wastage, digitalising production, and creating production systems that are flexible, adaptable, agile, and interoperable (Lampropoulos et al., 2019). Although IIoT can positively

impact 4IR, there are significant challenges, especially in terms of security. The following section looks at some of the major security concerns related to the emergence of IIoT.

5. Security concerns surrounding the emergence of IIoT

Since IIoT applications connect sensors, machines, and actuators in critical industries such as power grids, there are concerns that a security breach in IIoT applications can lead to devastating effects (Mumtaz, Alsohaily, Pang, Rayes, Tsang & Rodriguez, 2017). The emergence of IIoT security concerns is discussed in the following sub-sections.

5.1 Increased connectivity

The increased connectivity of IIoT systems creates several attack surfaces (Sadeghi, Wachsmann & Waidner, 2015). This is due to many connected technologies such as sensors deployed in the industrial sector, creating many access points for attackers to exploit. Therefore, IIoT systems increase the risk of exposure to cyberattacks for critical infrastructure (Paez & Tobitsch, 2017). IIoT systems are subject to physical attacks, such as hardware attacks, reverse engineering attacks, and side-channel attacks. IIoT software can also be compromised by runtime attacks, viruses, and Trojans. While communication protocols also have a risk of protocol attacks such as Distributed Denial of Service attacks (DDOS) and man-in-middle attacks (Koushanfar, Sadeghi & Seudie, 2012). IIoT applications are challenging to monitor daily, which is one of the reasons why there are several security vulnerabilities. Additionally, it is a challenge to notify users when there is a security breach, which can cause the breach to continue for an extended period without being detected (Paez & Tobitsch, 2018).

The interoperability capabilities of IIoT technologies are another security concern. Interoperability increases the scope of a data breach because the open and connected IIoT technologies make it easier for the damage from cyber-attacks to spread to other devices connected to the same network (Paez & Tobitsch, 2018). Many attacks against CI and CII have occurred in the past. An example is a cyberattack against a German Steel Mill. The attackers gained access to the CII systems by targeting the ICS devices through a phishing email. They further manipulated other systems on the network, which resulted in a system failure. Furthermore, the attackers caused physical destruction on the systems and prevented a safe shutdown on a blast furnace (Bajramovic et al., 2019).

5.2 Huge amounts of data

Another security IIoT security concern is the enormous amounts of generated data. IIoT applications connected to critical industries generate vast amounts of data processed in real-time. While this is an impressive ability of IIoT, there is a concern with how this data is stored (Yu & Guo, 2019). This data is often stored on cloud platforms, and with decreasing cost of cloud platforms, there is a broader number of IIoT applications storing their data on these cloud platforms. Storing this confidential data makes it attractive for cybercriminals to breach and get access to this sensitive data (Paez & Tobitsch, 2018). A data breach in these IIoT applications could cause devastating effects in the CIIs such as electrical power systems. Additionally, this data has to be often transferred from sensors to cloud platforms, introducing new cyber risks since attackers can also breach the data during transmission (Yu & Guo, 2019).

5.3 Legacy systems

Legacy systems are a serious concern for security in IIoT. Companies still use older systems known as Legacy systems because replacing them with new systems is disruptive and costly (Paez & Tobitsch, 2018). These companies then add a layer of IIoT applications on these Legacy Systems they use. Implementing IIoT devices on Legacy systems is a concern because attackers can find new ways to attack them (Bajramovic et al., 2019). Legacy systems are not designed for connectivity, and they are harder to secure (Paez & Tobitsch, 2018).

5.4 ICS security

Before IIoT devices were integrated into CII, most ICSs were isolated from the enterprise IT infrastructure (Yu & Guo, 2019). Merging CII with IIoT allowed ICSs to handle sophisticated environments (Bajramovic et al., 2019). The role of ICSs expanded from control and safety to providing processed information or responding to instructions from enterprise systems such as enterprise resource planning (ERP). However, the increased IIoT integration with ICSs creates cybersecurity risk concerns. IIoT exposes ICSs to cyber risks because of its highly

interconnected networks (Yu & Guo, 2019). These risks make finding appropriate and secure ways to integrate IIoT and ICS challenging (Bajramovic et al., 2019). As such, the following section discusses some approaches to secure IIoT systems.

6. Approaches for securing IIoT systems

Due to the number of security concerns of IIoT devices, several different approaches can be implemented to secure IIoT applications. Such approaches are discussed in the following sub-sections.

6.1 Data confidentiality protection

As mentioned in Section 5.2, the huge amounts of generated data can be breached during transmission and storage. Therefore, a solution to this issue would be data encryption, where the data is converted into a ciphertext for transmission and storage (Yu & Guo, 2019). However, traditional encryption algorithms cannot be applied because this would require downloading and decrypting the entire dataset (Spathoulas & Katsikas, 2019). As a result, more flexible encryption approaches have been proposed in the literature. He, Ma, Zeadally, Kumar, and Liang (2017) proposed a certificateless public key authenticated encryption with keyword search (CLPAEKS) for the Industrial Internet of Things where users can search for keywords in the ciphertext while also preserving privacy. The proposed CLPAEKS scheme specifically created for IIoT allows the data owner to encrypt a keyword and authenticate it. This means that an attacker cannot encrypt the keyword without the owner's private key, thus protecting the privacy and integrity of the data (He et al., 2017).

Traditional encryption approaches also suffer from a single point of failure. If the secret key is compromised, data confidentiality will also be compromised (Yu & Guo, 2019). A proposed approach by Mahalle, Prasad and Prasad (2014) solves this problem. The authors proposed threshold cryptography in IIoT systems where the key is divided into parts stored at different locations. This eliminates the single point of failure with the keys.

6.2 Network segmentation

Due to the connectivity of IIoT systems as mentioned in section 5.1. attackers could use other devices on the network to gain access to the industrial settings. A solution to prevent this would be to ensure that the IIoT systems are segregated in the network. This can be done where devices and sensors that manage other SCADA devices are on a separate network and not the same network as the IT infrastructure (Bajramovic et al., 2019).

6.3 Detection of attacks

It is important to implement approaches for detecting attacks to ensure the security of IIoT systems. Spathoulas and Katsikas (2019) describe using CNNs, Convolutional Neural Networks. CNNs can process huge amounts of data to detect anomalies in the functioning of industrial systems.

Another solution is the use of the Squeezed Convolutional Variational AutoEncoder (SCVAE) model. This solution makes use of low processing power, and it can detect the abnormal states of industrial systems (Kim, Yang, Chung, Cho, Kim, Kim, Kim, Kim, 2018). Additionally, SCVAE is a useful solution because it can also detect cyberattacks without using cloud solutions. Instead, the detection process takes place locally on the IIoT/ IoT network (Spathoulas and Katsikas, 2019).

6.4 Cyber-physical systems integrity

Since most IIoT systems are Cyber-Physical systems, the IIoT systems need to support the integrity verification of the Cyber-physical systems. A solution to this would be the use of attestation (Yu & Guo, 2019). Attestation is where the device that needs to be verified – called the prover – sends a status report of its software configuration to another device – called the verifier (Sadeghi, Wachsmann & Waidner, 2015). The prover does this to prove that it is in a trustworthy state. Although malicious software could forge the status report, the authenticity can be assured by trusted software and secure hardware (Yu & Guo, 2019).

6.5 Training employees

Most cyber-attacks are caused by human error. Therefore, to ensure that IIoT systems are secure, it is vital for the employees using IIoT systems to be trained in cybersecurity before gaining access to the IIoT system

(Bajramovic et al., 2019). The following section discusses how IIoT could transform our current understanding of CII.

7. How the Industrial IoT could transform critical information infrastructure

IIoT could change the way we understand Critical Information Infrastructures. The role of CIIs will no longer focus on managing and controlling CI. Instead, this role can expand where CII can also provide processed information. Additionally, IIoT could provide new ways for CIIs to control and manage CIs. For example, IIoT combined with CIIs could allow unmanned aerial vehicles to check oil pipelines to minimise workers' exposure to harmful chemicals in industries such as gas and oil (Agenda, 2015).

IIoT could also provide significant benefits for CII in the long run. From what was discussed in Section 3 paragraph 3, IIoT's use of real-time data can benefit CII. The data generated by IIoT devices can provide insights into the different CIs, such as power plants. Additionally, IIoT could transform how we think about CII processes, such as cost reductions, safety improvements, and increased efficiency. These potential benefits of IIoT could improve service delivery within nations.

Finally, IIoT could also transform the way we implement security for CII. Before the inception of IIoT, CII systems such as ICSs were thought of as isolated systems, and the connectivity brought by IIoT introduces new cyber security risks (Yu & Guo, 2019). This means that security measures previously applied to CII must change to accommodate the integration of IIoT. However, integrating ICSs with IIoT could also provide other challenges, such as increased research and development costs (Simon, 2017). This means that IIoT and CII integration could be challenging to implement due to the need for large investments to help initiate the integration.

8. Conclusion

Several topics were discussed in the aim to achieve the objective of this paper. The main critical points discussed were (1) understanding what IIoT means, (2) discussing where does IIoT fit within CII, (3) highlighting the impact of IIoT on 4IR, (4) discussing security concerns of IIoT in CII, (5) providing a few approaches to securing IIoT systems and (6) discussing how IIoT could transform CII.

While addressing the first critical point, the paper noted that IIoT can be seen as a subset of IoT that focuses on the industrial sector. Additionally, its use of sensors and other devices to obtain real-time operational data has shown that it can transform businesses. The second critical point could be seen in IIoT's ability to be integrated with CII. IIoT provides several benefits to ensure that CII can manage and control CI. IIoT improves CII efficiency, and cases of the integration of CII with IIoT have already been observed in nations such as the United Kingdom (Simon, 2017). To understand the third critical point, the paper noted that IIoT can be seen as one of the main drivers behind 4IR, and it meets the key 4IR requirements since the main aim of 4IR is digitalising the manufacturing industry.

It is important to note that security concerns have also been raised with the emergence of IIoT. The paper discussed this critical point by highlighting that the connectivity brought by IIoT will bring about new cyber risks. Additionally, the data collection and processing that comes with IIoT could create major concerns if the data were to be breached since it could contain vital information about a nation/business. The fifth critical point discussed in this paper highlighted a few approaches for addressing the noted security concerns. The approaches discussed were network segmentation, cyber-physical systems integrity and encryption. Finally, the paper discussed important aspects regarding how IIoT could transform our current understanding of CII. IIoT's ability to change the scope of CII, its security approaches, and providing additional benefits has shown that IIoT can positively transform CII.

References

Agenda, I. (2015) Industrial internet of things: unleashing the potential of connected products and services, World Economic Forum.

Arnold, C., Kiel, D. and Voigt, K.I. (2016) "How the industrial internet of things changes business models in different manufacturing industries", International Journal of Innovation Management, Vol 20, No. 8, pp 1-20.

Bajramovic, E., Gupta, D., Guo, Y., Waedt, K. and Bajramovic, A. (2019) "Security challenges and best practices for IIoT", INFORMATIK 2019 Workshops, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn.

Gilchrist, A. (2016). "Introduction to the industrial internet". Industry 4.0 , Apress, Berkeley, CA.

He, D., Ma, M., Zeadally, S., Kumar, N. and Liang, K. (2017) "Certificateless public key authenticated encryption with keyword search for industrial internet of things", IEEE Transactions on Industrial Informatics, Vol. 14, No. 8, 9 November, pp 3618-3627.

Jaidka, H., Sharma, N. and Singh, R. (2020) "Evolution of IoT to IIoT: Applications & challenges". Proceedings of the International Conference on Innovative Computing & Communications (ICICC),

Kim, D., Yang, H., Chung, M., Cho, S., Kim, H., Kim, M. and Kim, E. (2018). Squeezed convolutional variational autoencoder for unsupervised anomaly detection in edge device industrial internet of things. In 2018 international conference on information and computer technologies (icict), Dekalb, IL, USA.

Koushanfar, F., Sadeghi, A. R. and Seudie, H. (2012) "Eda for secure and dependable cybercars: Challenges and opportunities", Proceedings of the 49th Annual Design Automation Conference, June.

Lampropoulos, G., Siakas, K. and Anastasiadis, T. (2019) "Internet of Things in the context of Industry 4.0: An Overview". International Journal of Entreprenuerial Knowledge, Vol. 1, No. 7, June, pp 4-19.

Lopez, J., Setola, R. and Wolthusen, S. D. (2012) "Overview of critical information infrastructure protection", Critical Infrastructure Protection, Springer, Berlin, Heidelberg.

Magomadov, V. S. (2020) "The Industrial Internet of Things as one of the main drivers of Industry 4.0", IOP Conference Series: Materials Science and Engineering, Vol. 62, pp 1-4.

Mahalle, P. N., Prasad, N. R. and Prasad, R. (2014) "Threshold cryptography-based group authentication (TCGA) scheme for the Internet of Things (IoT)", 2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), Aalborg, Denmark, October.

Mcginthy, J.M. and Michaels, A.J. (2019) "Secure industrial Internet of Things critical infrastructure node design", IEEE Internet of Things Journal, Vol. 6, No. 5, 5 March, pp 8021-8037.

Mumtaz, S., Alsohaily, A., Pang, Z., Rayes, A., Tsang, K. F. and Rodriguez, J. (2017) "Massive Internet of Things for industrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation", IEEE Industrial Electronics Magazine, Vol. 11, No. 1, 21 March, pp 28-33.

Paez, M. and Tobitsch, K. (2017) "The Industrial Internet of Things: Risks, Liabilities, and Emerging Legal Issues", Exploring the Things in the internet of Things: Implications For Business, Consumers, and the Law, Vol. 62, No. 2, pp 217-247.

Pivoto, D. G., de Almeida, L. F., da Rosa Righi, R., Rodrigues, J. J., Lugli, A. B. and Alberti, A. M. (2021) "Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review", Journal of Manufacturing Systems, Vol. 58, January, pp 176-192.

Sadeghi, A. R., Wachsmann, C. and Waidner, M. (2015) "Security and privacy challenges in industrial internet of things", 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), IEEE, San Francisco, CA, USA, July.

Serpanos, D. and Wolf, M. (2017) "Industrial Internet of Thing", Internet of Things (IoT) Systems, Springer, Cham.

Simon, T. (2017) "Chapter seven: Critical infrastructure and the internet of things", Chapter seven: Critical infrastructure and the internet of things, Cybersecurity in a volatile world.

Sisinni, E., Saifullah, A., Han, S., Jennehag, U. and Gidlund, M. (2018) "Industrial internet of things: Challenges, opportunities, and directions", IEEE transactions on industrial informatics, Vol. 14, No. 11, 2 July, pp 4724-4734.

Spathoulas, G. and Katsikas, S. (2019). "Towards a Secure Industrial Internet of Things", Security and Privacy Trends in the Industrial Internet of Things, Springer, Cham.

Wan, J., Tang, S., Shu, Z., Li, D., Wang, S., Imran, M. and Vasilakos, A. V. (2016) "Software-defined industrial internet of things in the context of industry 4.0", IEEE Sensors Journal, Vol. 16, No. 20, 10 May, pp 7373-7380.

Yu, X., and Guo, H. (2019) "A survey on IIoT security", 2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS), Singapore, September.