A Primer on Industrial IoT and 5G: Implications and Challenges

Mohamadi Begum Y
Prof., Dept. of CSE
Presidency University
Bengaluru, India
Email: mohamadi.begum@presidencyuniversity.in

Clara Kanmani A
Assoc. Prof., Dept. of CSE
Presidency University
Bengaluru, India
Email:clara.kanmani@presidencyuniversity.in

Gopal K. Shyam
Assoc. Prof., Dept. of CSE
Presidency University
Bengaluru, India
Email: gopalkirshna.shyam@presidencyuniversity.in

ABSTRACT

The need for high-speed communication and flexibility are some of the key factors that have made the Industrial Internet of Things (IoT) a compelling technology. The availability of 5G mobile technology can help address these needs. This chapter aims to provide a comprehensive overview of the current state of research and solutions related to the IIoT, and 5G applications considering the original requirements and promises of these technologies.

Keywords—Industrial IoT, 5G

I. INTRODUCTION

Internet of Things (IoT) is a system that connects physical entities and devices including computers, networks, machines, sensors, etc. with an ability to exchange data with little or no human intervention. IIoT refers to the use of IoT Technologies in the industry sector for its operations. By harnessing IoT, industrial operations and processes not only improve productivity but also enhance operational efficiency at minimal operating costs. Market trends, global competition, and ever-changing customer expectations are a few factors influencing the use of IoT, in particular in the manufacturing industry. IIoT with its inherent potential enables industries to automate, optimize and control the environment with ease.

5G technology is a global wireless standard for broadband cellular networks. In comparison with 4G LTE networks, 5G offers higher speed, lower latency, and more capacity. Hence, 5G offers its clients access to more information faster and also businesses take advantage of such high connectivity benefits. As the number of connected IoT devices keeps increasing, the demand for bandwidth required for access and analysis is also increasing, which in turn is expected to be met by the 5G networks. It is imperative for the industries to gain an advantage from the combined 5G and IoT technologies for competing in the global market.

There is an exponential rise in the data collected from IoT devices whose storage and access challenges are addressed by the cloud. 5G supports distributed access concept which is a key advantage the cloud services can get through it. IIoT being a vital component of Industry 4.0 focuses on smart manufacturing and supply chain management using smart digital technology such as machine learning, big data, etc. By adopting 5G enabled IIoT practices, undoubtedly the industries get their reliability and communication requirements satisfied while there are few implications and challenges in the same.

This chapter is organized as follows: first, a background for the integration of IIoT with 5G and its impact on the industrial processes and operations is presented. Secure data storage and management apart from other challenges of 5G-enabled IIoT are discussed in the subsequent sections followed by future directions.

II. BACKGROUND AND RELATED WORK

The Industrial Internet of Things (IIoT) is a technology that enables the sharing of data and automation in the manufacturing industry. Highly digitized and connected production facilities in an industry are termed as ‘smart factories’ which are developed and driven by IIoT technologies. Such physical and computer components constitute cyber-physical systems in a smart factory and are used to monitor physical processes, and reproduce

the actual environment virtually. The cyber-physical systems are used to collect, process, and feedback data from various industrial endpoints.

IIoT is not just for manufacturing, but also has a wide range of applications including building project operations as detailed in [2]. The construction domain framework proposed in this paper intends to identify and debate the obstacles brought in by connectivity issues dominated by the influence of 5G technology. The cyber-physical systems are a vital part of the Industrial Internet of Things (IoT). They collect, process, and store data. That paper presents a case study that explores the potential of 5G technology to improve the efficiency of industrial IoT.

The three basic categories in information security often referred to as CIA (Confidentiality, Integrity, and Authenticity), are applicable for a majority of applications. However, the security requirements of each of these categories are no longer applicable to IoT and in particular to IIoT. With changing times, the CIA triad is no longer sufficient to confront emerging security concerns. Although more industrial IoT applications are emerging, IoT systems still lack a standardised broad layered structure. As mentioned in [3], the conventional strategy frequently uses three layers: the physical layer, the network layer, and the application layer.

Decentralized applications built on the IIoT platform's blockchain are intended to automate the creation of end-to-end manufacturing services. Users can control their production processes via smart contracts. The operation of IIoT-based businesses depends on these services.

The IIoT platform uses a blockchain to create decentralized applications that are designed to automate the production of end-to-end manufacturing services. Through smart contracts, users can manage their manufacturing operations. These services are necessary for the operations of IIoT-based businesses.

III. IMPLICATIONS

An IoT system is a composition of five major subsystems namely, sensors/devices, network connectivity, data management, a user interface, and a cloud environment. A cloud environment supports various IoT devices and applications with infrastructure, storage, and processing capabilities [16]. Further, the cloud ensures security aspects with appropriate authentication and encryption protocols.

IoT is ascending as the number of connected devices is set to increase from 700 million to 3.2 billion by 2023. Current networks lack the bandwidth to support the anticipated exponential growth. One of the vital factors adding to this rise is the evolution of 5G networks. The launch of 5G aids in performance improvement in terms of data transfer speed and reliability of connected devices, especially for connected devices like locks, security cameras and other monitoring systems which depend on real-time data updates.

There is expected to be a substantial improvement in smart manufacturing in IoT abilities by interfacing sensors on 5G to acquire real-time data about hardware execution [8]. When IIoT gets enhanced with machine learning and artificial intelligence, the information can be predicted, thereby avoiding critical equipment crashes. Further, particular hardware can be fixed through Augmented Reality support from remote experts empowered by high data transmission and low latency support of 5G.

Large amounts of data will be generated as a result of the deployment of applying IoT in power systems and is fundamental to understanding the association among various IoT devices [9]. For this scenario, 5G is giving considerable benefits to Power IoT (PIoT) with better opportunities. With IIoT [10], there is greater energy efficiency, reduced costs, better quality products, less hardware downtime and also significant improvement in decision making.

IV. CHALLENGES

With 5G, data transfer speeds will be faster than ever and thus increase efficiency and reliability. However, there are challenges in the adoption of IIOT such as failure to align key performance indicators with clear business objectives, improper organizational alignment, and IoT security threats [10]. As modern IoT gadgets go on the web and industrial facilities further mechanize various tasks, whole production lines may be adversely impacted in the event that a solitary sort of sensor becomes helpless against cyberattacks [11]. A modern Denial-of-Service (DoS) attack on such gadgets could impact and disrupt the entire system. There is a need for the developers to offer proper support and handle administration issues arising from such vulnerabilities.

Lots of challenges exist in IoT as well as IIoT [12]. Authentication, identification, and device heterogeneity are the security and privacy concerns in IoT. The major challenges are integrity, scalability, ethical communication mechanism, and business surveillance. In IIOT, as the devices are always turned on, they are visible to hackers leading to cyber vulnerability. In addition, there are no strong passwords and security protocols used. Outdated common code libraries are used and the firmware generally becomes obsolete.

There are deficiencies in the existing security patterns and testing of security pattern architectures [13]. Smart industries demand connectivity and interoperability to improve their performance which makes them

vulnerable to attacks. The research work in [14] proposes an IIoT attack taxonomy that aids in reducing the risks of such attacks.

V. FUTURE DIRECTIONS

There is a need for security, consistency, and accuracy in IoT. 2G and 3G networks are becoming obsolete while 4G to a certain extent supports HD video streaming and fast web browsing. 5G solves issues and challenges faced by smartphones and other smart technologies. 5G results in better performance as it uses a wide range of frequencies when it comes to connectivity. However, there are challenges in IoT and IIOT and there are blockchain-based solutions to counter these challenges.

5G and IoT are the two vital components for transforming how cities connect and operate. With IoT's boundless potential and 5G's faster speeds and low latency, these technologies leverage critical infrastructure for the future of connected communities. Nevertheless, scalability issues arising while building a design infrastructure to develop new applications enabled by 5G are still a concern [15].

IoT devices and 5G networks combined together are anticipated to intelligently detect and control traffic flows, keeping an eye on the state of the roads to ease traffic congestion. The use of connected devices in cities and buildings to track, monitor, and manage energy is greatly facilitated by 5G.

As we move forward, 6G (sixth-generation wireless) is the successor to 5G cellular technology. In the future, 6G networks will be able to utilize higher frequencies than 5G networks and provide substantially higher capacity and much lower latency for various applications.

VI. CONCLUSION

IoT devices engaged in industrial operations are vulnerable to cyberattacks which may create gaps in the overall manufacturing process and sometimes result in catastrophic effects on the rest of the system. Further, data management for 5G networks and dependency on the cloud are critical for the effectiveness of IoT-enabled industrial needs. These challenges when addressed will definitely aid IIoT to take full advantage of the emerging 5G network technologies.

REFERENCES

[1] Rao, S.K.; Prasad, R. Impact of 5G Technologies on Industry 4.0. Wirel. Pers. Commun. 2018, 100, 145–159, doi:10.1007/s11277-018-5615-7.

[2] Reja, V.; Varghese, K. Impact of 5G Technology on IoT Applications in Construction Project Management. ISARC. Proc. Int. Symp. Autom. Robot. Constr. 2019, 36, 209-217, doi:10.22260/ISARC2019/0029.

[3] Varga, P.; Plosz, S.; Soos, G.; Hegedus, C. Security threats and issues in automation IoT. In Proceedings of the IEEE 13th International Workshop on Factory Communication Systems (WFCS), Trondheim, Norway, 31 May–2 June 2017.

[4] Alladi T., Chamola V., Parizi R., Choo K.K.R. Blockchain Applications for Industry 4.0 and Industrial IoT: A Review. IEEE Access. 2019; 7:176935–176951. doi: 10.1109/ACCESS.2019.2956748. [CrossRef] [Google Scholar]

[5] Wang Q., Zhu X., Ni Y., Gu L., Zhu H. Blockchain for the IoT and Industrial IoT: A Review. Internet Things. 2019:100081. doi: 10.1016/j.iot.2019.100081.

[6] Chen W., Ma M., Ye Y., Zheng Z., Zhou Y. IoT Service Based on JointCloud Blockchain: The Case Study of Smart Traveling; Proceedings of the 2018 IEEE Symposium on Service-Oriented System Engineering (SOSE); Bamberg, Germany. 26–29 March 2018; pp. 216–221.

[7] Bai L., Hu M., Liu M., Wang J. BPIIoT: A light-weighted blockchain-based platform for Industrial IoT. IEEE Access. 2019;7:58381–58393. doi: 10.1109/ACCESS.2019.2914223.

[8] https://www.wipro.com/infrastructure/the-impact-of-5g-on-iot-in-manufacturing/

[9] J. Tao, M. Umair, M. Ali and J. Zhou, "The impact of Internet of Things supported by emerging 5G in power systems: A review," in CSEE Journal of Power and Energy Systems, vol. 6, no. 2, pp. 344-352, June 2020, doi: 10.17775/CSEEJPES.2019.01850.

[10] https://www.iotforall.com/industrial-iot-benefits-use-cases-and-challenges-of-wide-spread-iiot-implementation

[11] https://www.forbes.com/sites/forbesbusinesscouncil/2021/10/15/challenges-to-5g-networks-from-iot-devices/

[12] X. Yu and H. Guo, "A Survey on IIoT Security," 2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS), 2019, pp. 1-5, doi: 10.1109/VTS-APWCS.2019.8851679.

[13] K. Shaukat, T. M. Alam, I. A. Hameed, W. A. Khan, N. Abbas and S. Luo, "A Review on Security Challenges in Internet of Things (IoT)," 2021 26th International Conference on Automation and Computing (ICAC), 2021, pp. 1-6, doi: 10.23919/ICAC50006.2021.9594183

[14] A. C. Panchal, V. M. Khadse and P. N. Mahalle, "Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures," 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), 2018, pp. 124-130, doi: 10.1109/GCWCN.2018.8668630.

[15] G. P. Fettweis, "5G and the future of IoT," ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference, 2016, pp. 21-24, doi: 10.1109/ESSCIRC.2016.7598234.

Lynn, T., Endo, P.T., Ribeiro, A.M.N.C., Barbosa, G.B.N., Rosati, P. 2020; The Internet of Things: Definitions, Key Concepts, and Reference Architectures. In: Lynn, T., Mooney, J., Lee, B., Endo, P. (eds) The Cloud-to-Thing Continuum. Palgrave Studies in Digital Business & Enabling Technologies. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-41110-7_1