IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

APPLICATIONS OF AN INDUSTRIAL INTERNET OF THINGS BASED ON THE PERSPECTIVE OF CYBER-PHYSICAL SYSTEMS

Nandini Gargula,Computer Network and Systems Engineer

INFORMATION TECHNOLOGY,Charles Stuart University

Sydney Australia,

ABSTRACT

In the context of industrial production settings, the "Industrial Internet of Things" is an acronym for "Industrial Internet 4.0," which refers to the integration of massively deployed smart computer and network technologies in order to achieve the goals of automating, ensuring reliability, and controlling processes (I-IoT). When it comes to increasing productivity, efficiency, safety, and intelligence in the manufacturing system environment, I-IoT is primarily concerned with the implementation of the Internet of Things (IoT), which allows anything, anywhere, and at any time to be connected. When compared to consumer IoT, I-IoT has a number of distinct characteristics and requirements, including the unique types of smart devices that are incorporated, network technologies and quality-of-service requirements, and stringent requirements for command and control and command and control infrastructure. Throughout this article, we perform a comprehensive analysis of the corpus of existing research on I-IoT in order to provide a consistent appraisal of the technology from a systems viewpoint and to better understand the complexity of the I-IoT and its special demands and requirements. In this section, you'll learn about the Internet of Things architecture, as well as about its applications (such as industrial automation and process automation), and its characteristics.

1. INTRODUCTION

Digitalized systems that are capable of sharing process characteristics, operational status, and availability to collaborate with other equipment or humans are part of the Industry 4.0 trend. A smart value chain is one in which every node in a product's chain is equipped with decision-making skills and methods of communication, allowing for the exchange of useful information between nodes in the chain (Kagermann et al. 2013). Connectivity technologies like Internet of Things (IoT) and Internet of Services (IoS) are crucial for manufacturing environments to have a comprehensive view of their current status (Gilchrist 2016).

Modern embedded systems' increased processing power and the advent of CPS have enabled the development of a new form of networked control system for factory automation. To replace the existing automation pyramid and unite the traditionally separate fields of information technology (IT) and operational technology (OT), CPS integrates IoT and automation technologies (Monostori et al., 2016). The first focuses on the manipulation of data in order to get relevant insights. During the manufacturing process, this refers to the support of the formation of physical value. The digital integration of traditional software systems, such as ERP and factory execution systems, is one illustration of this integration (MES). Building blocks of a smart factory are defined by CPS, which will be central CPPS of Industry 4.

Industrial systems are naturally heterogeneous in terms of software, which presents a fundamental obstacle to digital integration. In many modern firms, third-party or custom-built digital applications that are either part of a legacy system or a combination of the two are essential. Developing business applications is a complex endeavour, and constructing a single application capable of running an entire organisation is practically impossible (Hohpe and Woolf 2004). There is only a limited amount of functionality that ERP systems can give despite the fact that they are widely used. ERP systems Regardless, modern industrial systems necessitate or even benefit from component heterogeneity (Lin and Miller 2016). It is possible to take advantage of the advantages of different distributors by purchasing components from different manufacturers. In addition, as technology continues to advance, new components must be added to existing systems. Different standards and laws may mandate specific solutions that are neither scalable or convenient for usage in all situations.

2. LITERATURE REVIEW

Industry 4.0 security research thus far has shown [1–3] that IIoT devices are also vulnerable to vulnerabilities, painting a similarly grim picture of existing IIoT deployment security. The availability or operational safety of industrial infrastructure can be seriously compromised in a targeted attack, and this can have severe consequences. German steel industry in 2014 and Ukraine power grid in 2015 are two instances of recent attacks [4, 5]. Breakdowns have the potential to harm not just the organisation that is experiencing them, but also its customers and suppliers, as well as a country's critical infrastructure as a whole.

To put it another way, industrial locations have different security challenges than residential ones. As an example, industrial gadgets have a much longer lifespan than consumer devices, therefore they require more security measures and longer-term patch maintenance. In the same way, industrial IoT networks tend to be far larger than consumer IoT networks, which often only include a few devices. Deploying a segregated secure network architecture becomes more difficult as the number of services provided increases.

Various solutions have been offered, such as [6]–[9], in order to counteract the attacks outlined. In light of these findings, we've developed a taxonomy for IoT security protocols that divides them into four categories: Access control, privacy protection, and user/device authentication are all part of the key management process. They are depicted in Fig. 1 in connection to the IoT reference layers as well as the attacks.

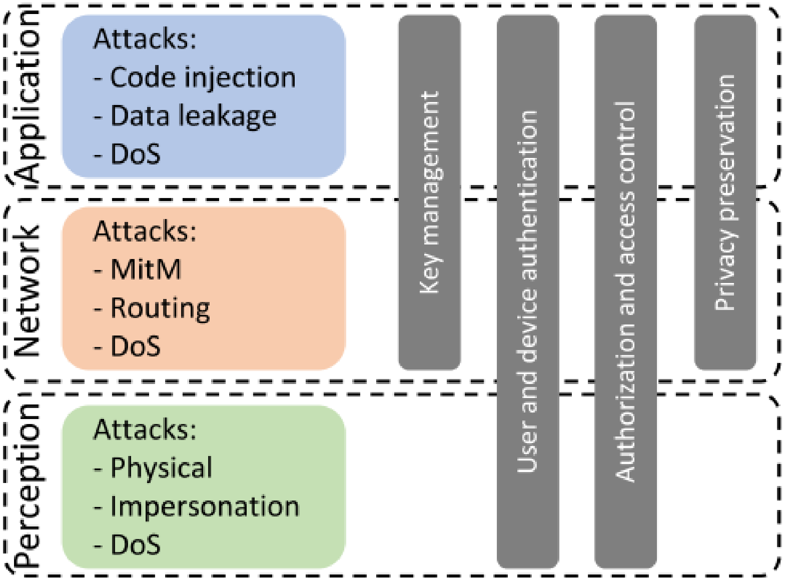

Fig. 1. A diagram of the Internet of Things (IoT) reference levels, showing threat categories and countermeasures.

1) IoT deployments present a challenge to key management because of their scale and heterogeneity. However, public-key schemes are easier to handle but demand more computational resources than symmetric schemes in general.

2) Authentication of users and devices is a way to verify that the people or things you are dealing with are who they say they are. When it comes to user authentication, it's common to use numerous factors. Contextual information, such as fingerprints, can be applied to gadgets as well.

3) Users and devices can only access resources and services if they have been authorised and have the proper credentials. Rules and regulations, for example, can be used to accomplish this, but they rely on authentication in order to do so.

4) Protection of sensitive personal information, such as medical records, from outsiders is known as privacy preservation. Secure multiparty computations, as well as encryption of information and transmission, are all part of this [10].

3. ARCHITECTURE FOR CYBER-PHYSICAL MANUFACTURING CONTROL SYSTEM

3.1. The evolution of the system

A typical modern factory employs a series of production lines. Orders generated via reseller chains are monitored by the ERP system, which then issues production-level orders via the MES to build the necessary quantities to fill those orders. Production is initiated by the MES, and the ERP system receives updates on the progress of the production. There are various flaws in the notion of Industry 4.0 that must be taken into account.

- As long as a single resource fails, the entire manufacturing line fails as well.
- It is tough to grow and reconfigure a manufacturing line since the MES and machine may have a large number of interface possibilities.
- In some cases, real-time updates to the ERP system from the MES are not possible.

Industrial control systems are usually expensive and time-consuming to design, maintain, and change. The lack of re-configuration comes from being unable to respond quickly to emergencies (change and unexpected disturbances). This study looks at a distributed, intelligent control system with nodes that work together to complete more than one task. Dynamic market needs necessitate flexible, reconfigurable, and reusable technologies.

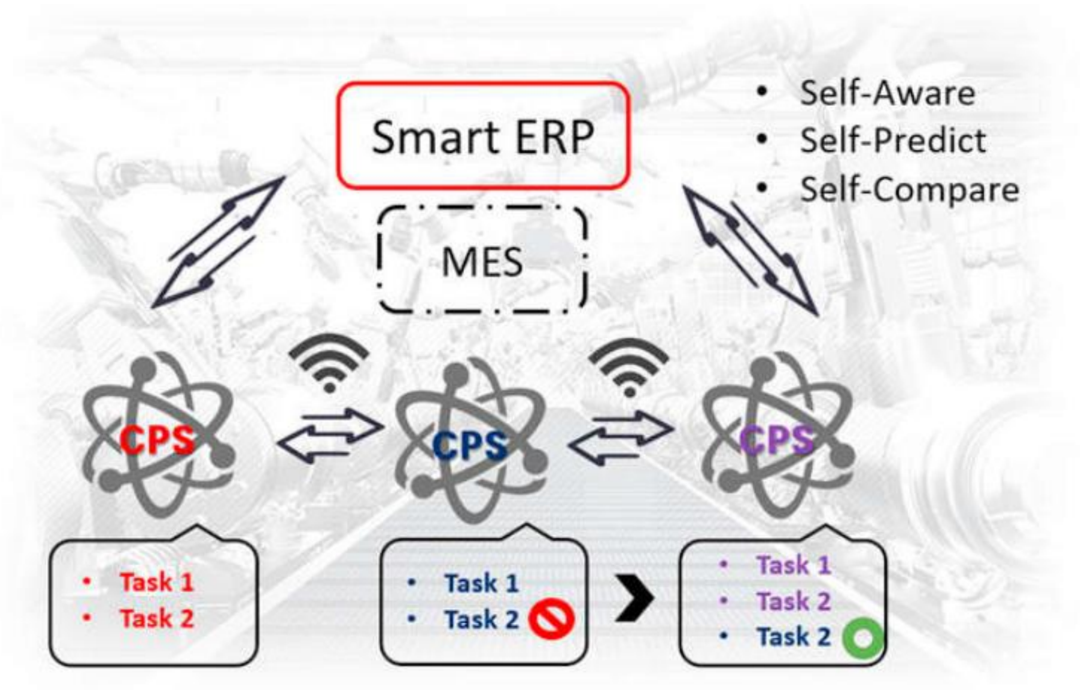

Fig. 2. Architecture for cyber-physical systems in manufacturing.

Replacement of the serial manufacturing line with CPS machines is depicted in Fig. 2. With sensors and wireless radio connectivity, a failing machine can be replaced by a working one. Precision and predictive data can be generated by the sensor. In the same way, machine sensors can be self-aware, self-predict, and self-compare through their controllers. Collaborative problem solving through a machine's ability to self-diagnose, check the current status of the production line, and then respond accordingly. Another possible point of failure is eliminated because machines communicate directly with each other without the need for a MES. In order to deal with the issue of interface mismatch and reconfiguration.

3.2. Main architecture

By utilising the Industrial Internet of Things, this design aims to create Cyber-Physical Systems. This architecture relies heavily on the industrial Micro Control Unit (MCU) depicted in Fig. 3. Data sources, actuators, and equipment are all connected to a microcontroller (MCU). The cloud/fog computing platform and the MCU communicate back and forth to exchange data and control commands. Data can be transmitted via this media. Anomaly detection and system optimization are all possible with Fog Analytics, which collects, processes and analyses data from a wide range of edge devices for analysis, machine learning and anomaly detection. Making use of knowledge ontology analytics and reasoning in the cloud platform lets the cyber world recognise real-world scenarios and problems. So, in the cyber realm, you can take precautions or make predictions that can then be used in the real world.

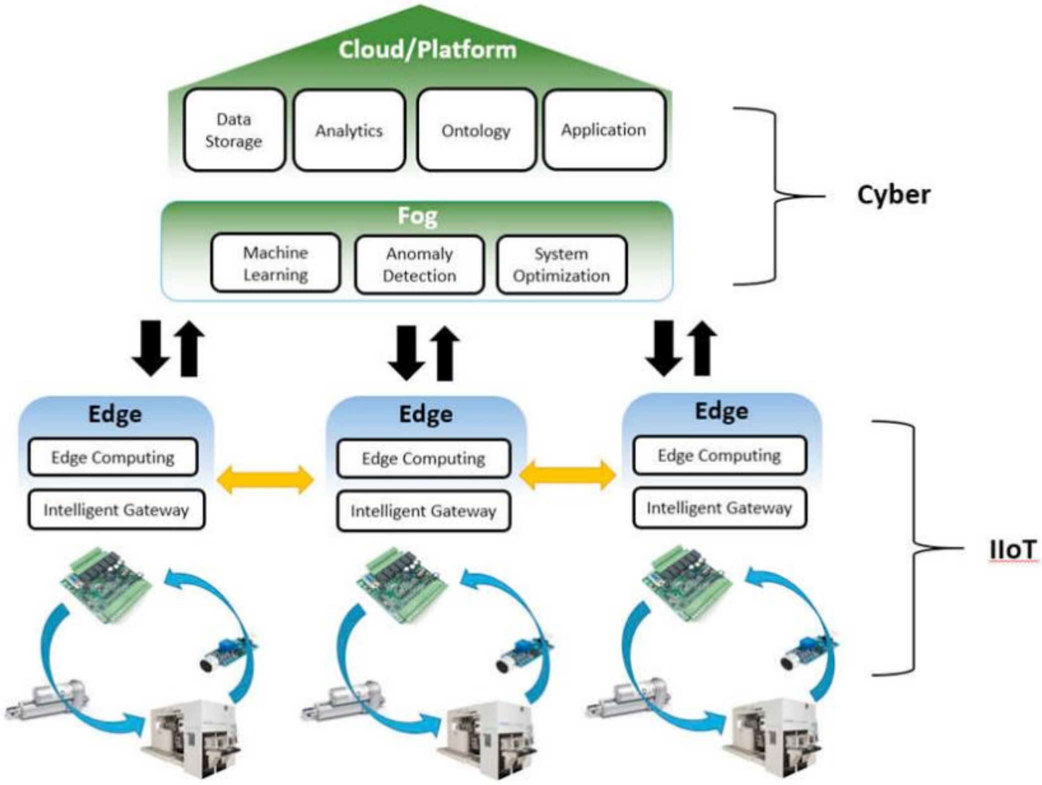

Fig. 3: CPS Architecture based on Multi-MCU and several technologies.

In this design, the main functions of MCUs are:

• Interworking of information: Using wireless radio links, the machines may communicate with one another and take over the functions of a malfunctioning unit when deployed by the MCU. Another possible point of failure is eliminated because machines communicate directly with each other without the need for a MES.

• Intelligent gateway: Gateways connect existing and new systems, allowing data to travel between the edge and the cloud in a secure and seamless manner. Data sent to the cloud by connected devices can be monitored, analysed, reported on, and alarms can be generated depending on this information.

•Edge computing: MCU software can be used to implement edge computing. The AWS IoT Greengrass Core may be accessed directly, which is more efficient. For this reason, AWS provides pre-configured hardware and software. While still relying on the cloud for management, analytics, and long-term storage, AWS IoT Greengrass devices can respond to local events quickly. [19] Using the AWS IoT Platform, Greengrass allows connected devices to perform AWS Lambda tasks, execute machine learning models predictions, and maintain device data in sync.

4. RESULTS AND DISCUSSION

Although the IIoT is a critical component of the I4.0, it is prone to a wide range of security threats. To keep IIoT infrastructure safe from cyber-attacks, a lot of work has been done. All possible cyber-attacks and responses must be examined in order to protect this critical infrastructure against cyber-attacks.

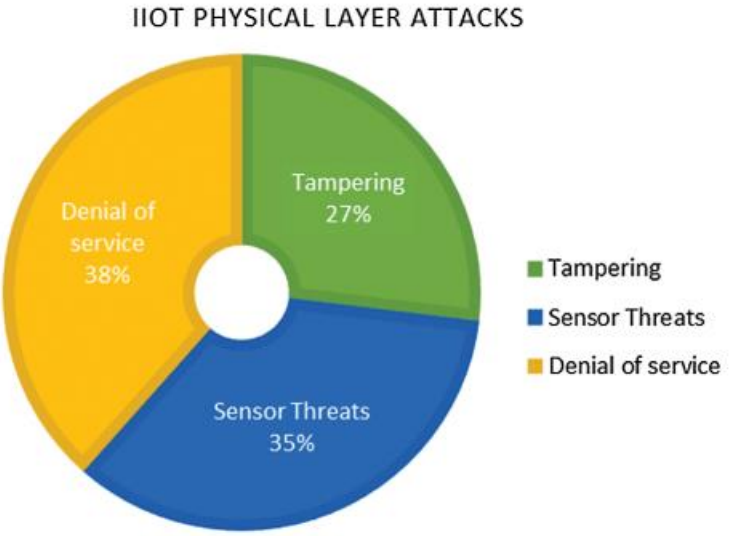

Figure 4: CS attacks targeting the application layer of IIoT.

Individuals and businesses alike should take the necessary precautions to safeguard their investments, as evidenced by the aforementioned data. An effective network defence strategy includes the use of security solutions, adequate management and deployment.

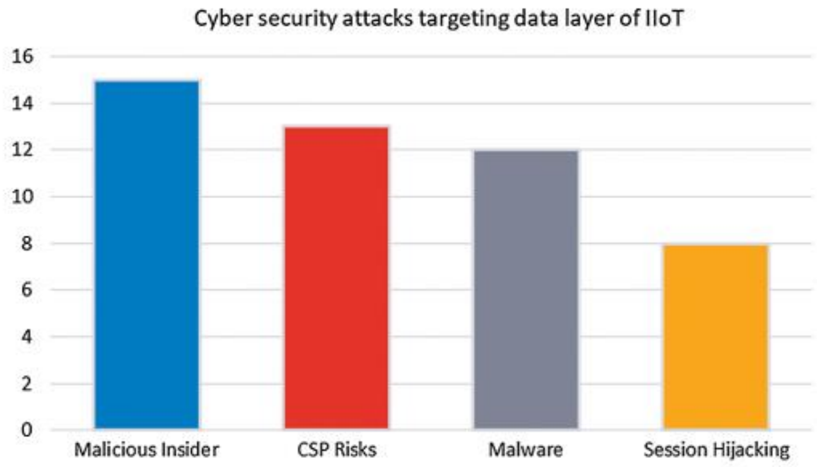

Figure 5: CS attacks targeting the Data layer of IIoT

DoS, information extraction, and privileged execution are all methods used by malicious insiders to attack this layer.. People and businesses alike need to put in place strict security measures, and their personnel need to be educated about the importance of protecting themselves. These threats necessitate the use of limited privileges and the separation of duties to protect the data layer from these risks. If suitable security precautions aren't taken, most large enterprises rely on cloud services for data storage.

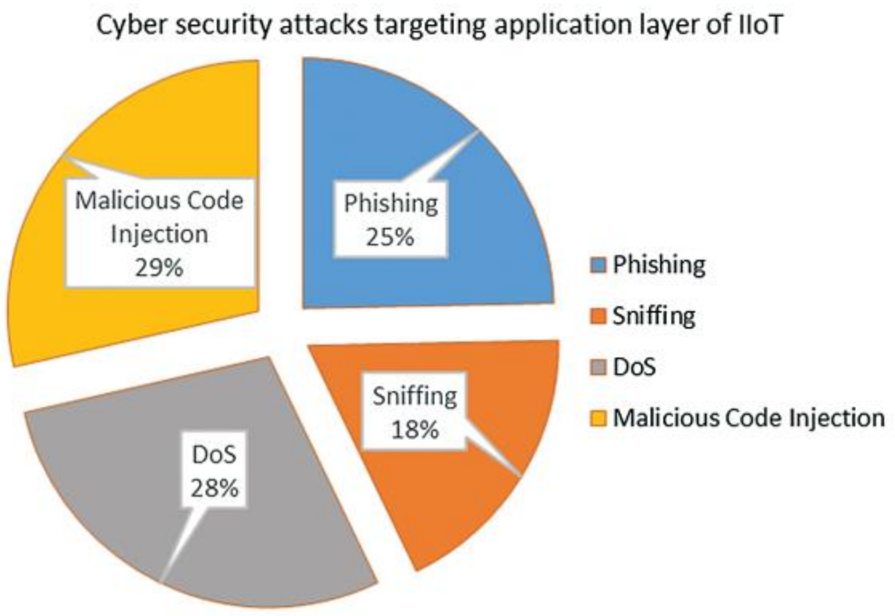

Figure 6: CS attacks targeting the application layer of IIoT.

CONCLUSION

I-IoT architecture, applications, and characteristics as well as current research efforts on control, networking, and computing systems in I-IoT have been presented in this study. Additionally, problems and future research needs have been addressed. Examples of I-IoT applications include process automation and factory automation (FA). Application layer, communication layer, and physical layer are all part of I-IoT architecture (FA). Aspects of I-IoT applications include their number of nodes, cycle time, and dependability. IoT systems have been examined from the viewpoints of control, networking, and computing architecture. We've looked into industrial control architectures with centralised, decentralised, and hierarchical control systems. The threat of CS attacks is one of the most pressing issues facing I4.0. These attacks, as well as their possible outcomes and countermeasures, have been discussed in detail in order to address this issue. IoT architecture and possible attacks on each layer of IIoT are examined in this extensive review of literature. Researchers and practitioners in the IIoT will benefit from this by being more aware of potential threats and solutions. According to a comprehensive study that examines current IIoT-related cyber-security and privacy issues, a framework has been developed to provide an overview of potential threats to security and privacy as well as attack methods and countermeasures.

REFERENCES

[1] J. Wurm et al., “Security analysis on consumer and industrial IoT devices,” in Proc. ASP-DAC, Jan. 2016, pp. 519–524.

[2] A. Sadeghi, C. Wachsmann, and M. Waidner, “Security and Privacy Challenges in IIoT,” in Proc. ACM/EDAC/IEEE Des. Autom. Conf., Jun. 2015, pp. 1–6.

[3] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, “Industrial Internet of Things: Challenges, opportunities, and directions,” IEEE Trans. Ind. Informat., vol. 14, no. 11, pp. 4724–4734, Nov. 2018.

[4] R. M. Lee, M. J. Assante, and T. Conway, “German Steel Mill Cyber Attack,” Ind. Control Syst., vol. 30, 2014, Art. no. 22.

[5] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, “Ukraine cyberinduced power outage: Analysis and practical mitigation strategies,” in Proc. IEEE 70th Annu. Conf. Protective Relay Eng., Apr. 2017, pp. 1–8.

[6] K. T. Nguyen, M. Laurent, and N. Oualha, “Survey on secure communication protocols for the Internet of Things,” Ad Hoc Netw., vol. 32, pp. 17–31, 2015.

[7] M. Frustaci, P. Pace, and G. Aloi, "Securing the IoT world: Issues and perspectives," in Proc. IEEE Conf. Standards Commun. Netw., Sep. 2017, pp. 246–251.

[8] A. K. Das, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for Internet of Things," Future Gener. Comput. Syst., vol. 89, pp. 110–125, 2018.

[9] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," J. Inf. Secur. Appl., vol. 38, pp. 8–27, 2018.

[10] V. Oleshchuk, "Internet of Things and privacy preserving technologies," in Proc. Int. Conf. Wireless Commun., Veh. Technol., Inf. Theory Aerosp. Electron. Syst. Technol., May 2009, pp. 336–340.

[11] M. Humayun, N. Jhanjhi, B. Hamid and G. Ahmed, "Emerging smart logistics and transportation using IoT and blockchain," IEEE Internet of Things Magazine, vol. 3, no. 2, pp. 58–62, 2020.

[12] M. Humayun, N. Jhanji and M. Alamri, "Smart secure and energy Efficient scheme for E-Health applications using IoT: A Review," International Journal of Computer Science and Network Security, vol. 20, no. 4, pp. 55–72, 2020.

[13] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb and S. Mahmood, "Cyber security threats and vulnerabilities: A systematic mapping study," Arabian Journal for Science and Engineering, vol. 45, no. 4, pp. 3171–3189, 2020.

[14] R. von Solms and J. van Niekerk, "From information security to cyber security," Computers & Security, vol. 38, no. 6, pp. 97–102, 2013.

[15] R. Hill, "Dealing with cyber security threats: International cooperation, ITU, and WCIT," in Proc. ICCC, Tallin, Estonia, pp. 119–134, 2015.

[16] D. Craigen, N. Thibault and R. Purse, "Defining cybersecurity," Technology Innovation Management Review, vol. 4, no. 10, pp. 1–9, 2014.

[17] A. Humayed, J. Lin, F. Li and B. Luo, "Cyber-physical systems security–A survey," IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1802–1831, 2017.

[18] B. Bordel, R. Alcarria, T. Robles and D. Marten, "Cyber physical systems: Extending pervasive sensing from control theory to the internet of things," Pervasive and Mobile Computing, vol. 40, no. 2, pp. 156–184, 2017.

[19] G. Erboz, "How to define industry 4. 0: the main pillars of industry 4.0," in Proc ICoM 2017, Nitra, Slovakia, pp. 1–2, 2017.

[20] M. Humayun, N. Jhanjhi, M. Alruwailli, S. Amalathas, V. Balasubramaniam et al., "Privacy protection and energy optimization for 5G-aided industrial internet of things," IEEE Access, vol. 8, no. 1, pp. 183665–183677, 2020