Journal of Engineering and Technology

ISSN 2180-3811 eISSN 2289-814X https://journal.utem.edu.my/index.php/jet/index

REVIEW ON IOT SECURITY AND CHALLENGE IN INDUSTRY 4.0

Nurul Nuraini Abdullah*[1] and Mohamad Fadli Zolkipli[2]
[12] School of Computing, University Utara Malaysia, Sintok, 06010, Kedah, Malaysia.
n_nuraini_abdullah@soc.uum.edu.my

Article history:
Received Date: 2021-05-12
Accepted Date: 2021-06-23

Keywords:
Internet of Things, Wireless network, Security threats, Privacy protocols, IoT networks

Abstract— Wireless networks are very exposed to the danger of security. The majority of in military, commercial, health, retail, and transportation wireless communication network are used. These systems utilize networks that are wired, mobile, or adhoc. The Internet of Things (IoT) was quite attractive. The future of the Internet is regarded by IoT. In the future, IoT plays an important part and affects our way of life, norms, and business methods. IoT use is predicted to expand quickly in the next years in many applications. The IoT provides for the connection and information sharing of billions of equipment, people, and services. As IoT devices are being used more widely, several security threats are occurring in the IoT networks. In order to provide privacy, authentication, access, and integrity control, it is crucial to implement

efficient protocols for the security of IoT networks and privacy among others. In addition, user privacy in the IoT environment is becoming critical since much personal information is provided and distributed among related items. It is, therefore, necessary to guarantee that personal data are protected and controlled from cloud events. The presentation addresses security and privacy dangers and concerns coming out of IoT services and presents ways to the industrial problem of security and privacy. In this article, a study on security and problems in IoT networks are discussed.

I. Introduction

In this modern era, connecting every moment of things embedded with electronics, software, and sensors to the internet enabling to collection and exchange of data without human interaction called the Internet of Things (IoT) [1]. It has emerged as one of the most significant developments of the twenty-first century. It likes now we can use embedded devices to attach everyday tools we use such as kitchen appliances, vehicles, and many more connected to the internet that allows for communication between people, processes, and items. Several devices have been developed which are being utilized as IoT, such as, Laser Scanner, Radio Frequency Identification Devices (RFID), Infrared Sensor, Global Positioning System (GPS), etc. [2]. With the RFID and wireless IoT, we have control over our daily life. Today IoT is widely useful for social life devices such as smart homes, transit, smart grids, security, training, fitness, health, environmental monitoring, and so on. In 2016, a DNS service provider Dyn faced a severe Distributed

Denial of Service (DDoS) attack, which caused an interruption in service of various popular websites like Amazon, Facebook, and Twitter [2]. Users should be ensured that they do not longer have unauthorized access if an IoT layer has been targeted and the hackers may simply reach the compromised node. In addition, viruses, malware, and hackers can damage the integrity of information and data that threatens the entire IoT system publicly. IoT security domain is intriguing and vibrant. Looking at the safety aspect, various flaws are there in IoT architecture. In most IoT structures, Wireless Sensor Network (WSN) and IP based Wireless Sensor Network are vulnerable and security risks [2]. If a node is hacked, false persons can get information and harm the entire system significantly.

Global web traffic through these devices was predicted by Cisco to reach 49 Exabytes of traffic by 2021, in contrast to 2018's 17 Exabytes [12]. This is not unexpected, as each of the services offered by a particular provider or a subscription the customer requested might operate on each device. Gartner predicts that over a quarter of all cyber-attacks against businesses will be IoT-based by 2025 [13]. However, comfort and economy on the market are rarely designed over safety. In addition, in aged firmware or designs there is a general lack of defense. Similarly, the promotion of user awareness and education takes minimal account. For example, both John Deere and UPS are already using IoT-enabled fleet tracking technologies to cut costs and improve supply efficiency [14]. Before the advent of the IoT, information leakage and denial of service was the most security threats reported but with IoT, security threats have gone far beyond the theft of information or denial of service [16]. These dangers may now be connected, even physical security, to real life. A lot of personal information is exchanged in an IoT network and supplied across linked devices, which also poses privacy problems.

The internet communication of all objects with computers, sensors, and electronics allows data to be gathered and exchanged without interference by humans, identified as IoT. Beginning with cognitive IoT, which decided actions based on the generated data, it then moved on to IoT 2.0, which made way to human communication in devices [3]. It means that IoT already exists before and has been used in education. But at that time not many people know about IoT until it becomes famous day by day until now. Each provenance had to make software, sensors, and connectivity which enables these things to connect and change data [4]. All IoT devices must be linked to the Internet so that they can change data and do what devices that used IoT need to do. The separation between physical and digital industries is now consigned to the past because the IoT makes possible hybrid solutions that merge physical products and digital services [5]. The use of IoT in the industry will help to solve the issue of physical and digital industries being separated. The number of physical objects connected to the Internet constantly grows and a common thought says the IoT scenario will change the way we live and work [7].

IoT systems involve different platforms, data, and devices, and the continuous change because of mobility [6]. So, it is not easy to find solutions for the problem related to IoT security. IoT objects are vulnerable to various security threats that may lead to data leakage or exploitation, as most internet-connected computers. While the industry has been aware of the security issues, recent high-profile cyberattacks, such as the one on DYN's infrastructure which exploited 100, 000 infected IoT devices [8]. Even the industry has been aware of the security issues but the number of cyberattacks still increased when using IoT devices. Some of the IoT applications are used to monitor high-security infrastructures such as the smart grid and hazardous material production facilities [9]. The number of different devices

related to IoT networks arises, safety vulnerability capability will increase exponentially.

This article is organized and divided into six parts which are Section I introduction for IoT security and challenges in Industry 4.0, while Section II is divided into two parts which are the security attacks for different layers in IoT and measures of security attacks in IoT for Industry 4.0. Section III discusses the IoT applications. Section IV is the conclusion of the topic for this article. Also have in Section V is acknowledgment and references that been used for this article in Section VI.

II. Security attacks for different layers in IoT and measures of security attacks in IoT for Industry 4.0

This part will explain the security in IoT and measures of IoT in Industry 4.0.

A. Security attacks for different layers in IoT

For the IoT services, there are numerous types of things from light to rich devices; the communication between things occurs through various networks [11]. Various safety issues threaten data confidentiality and likely actions on each layer. The security attacks for the different layers are:

1. Layer of physical

The physical layer is made of a few capable sensor technologies for various sorts of attacks such as GPS, Zigbee, and Bluetooth. This kind of attack is being carried out for the IoT hardware components and the opponents the IoT system must be near.

- **Network Node Wireless Sensor interruption**

This type of attacker gets involved in radio frequencies of wireless sensor nodes and then afterward it blocks the signals which stop the communication of nodes [10]. If an attacker manages blocking in critical sensor nodes successfully, it could suspend IoT services. DoS attacks can influence RF transmissions with numerous noisy signals that interrupt the RF network.

- **Injections for malicious code**

The opponent can put the malicious program in a node physically and use that attack in a node to access the complete IoT system. An attacker places a plug and player in a node, for instance, and provides complete access to that node, and controls the entire IoT system.

- **Eavesdropping**

The attacker can readily access personal information such as a password or other information that runs from tag to user or from user to tag. This type of attack can happen because RFID has wireless characteristics [10].

- **Spoof**

When you spoof the opponent, he broadcasts fallacious information on the RFID system and thinks it to be original. This allows the attacker to gather data and access the network fully.

- **Attack Timing**

Another danger to system confidentiality is the time attack in which the cryptography key may be obtained by examining the time necessary for encryption. Side Channel is also an attack on an opponent when the data on operations is leaked, for instance, power consumption, treatment, or electromagnetic radiation, attacks the encryption device.

2. Layer of network

When the network attack takes place, the opponent should focus on the system IoT network, and the IoT network should not be near the attacker.

- **Attack of Traffic Analysis**

When any web browser is used, the major security threat is the traffic analysis attack. The adversary can access secret information and other useful data which are from RFID technology because of its wireless attribute [10]. The attacker first receives network linked information and details before conducting this attack. The task is done through sniffing, such as application port scanners, packet sniffing, and so on.

- **Attack of the Sleep Default**

The sensor nodes in the wireless system are charged with

batteries that are incompatible because battery life is not very efficient so that the sleeping schedule is employed to improve battery life. The opponent wakes the battery during an attack in sleep deprivation that leads to higher consumption of the battery.

- **Unapproved Access to RFID**

In RFID systems it is quite easy for anybody to access tags because most of them lack the set protocol or any authentication method in the RFID system. It shows clearly that an attacker may edit, read, or delete sensor node information.

- **Attack from Man in the Middle**

The adversary might have access to secret information that violates privacy between nodes through monitoring, network monitoring and interferes with communicating with two sensor nodes. Unlike physical attack types, an attacker must not be near physically but must concentrate at the layer of the network on connecting nodes inside a network protocol.

- **Service Denial**

The attacker can attack the IoT network by delivering a lot of traffic data while it denies service attacks. It manages all data which leads to a settled attack denial. In this kind of attack, the user cannot access their resource through the network.

3. Layer of processing

The processing layer includes several kinds of technologies, for example, data recovery and data processing. Cloud Attack is the most important type of IoT system attack and network security issue.

- **Unlicensed to Access**

Layer processing provides storing of data and several functions for the processing of applications. This attack allows the opponent to access system functions easily by allowing them to delete important information that might do a great deal of IoT network damage.

- **Security Application**

Service software (SAAS) provides cloud software available and information through the Internet, in the context of application security. The opponent of the IoT system might simply steal data and do harmful operations over the Internet. Open Web Application Security Project (OWASP) has identified many web services and security issues in SAAS [10].

- **Safety Infrastructure**

The Services Platform (PaaS) allows developers not to access the underlying layer and providing service providers are responsible for the safety. The developer's objective is to keep IoT safe, yet lower-level security stays exposed and leads to vulnerability.

- **Virtualization Threats**

The security of the virtual machine is very crucial since other computers affect the damage to the system. Virtual machine security is particularly significant as other computers are affected by machine damage [10].

- **Shared Resources**

The same sharing of resources and use in virtual machines might lead to different security dangers in IoT networks. The opponent monitors all the resources shared through covert channels between virtual equipment. So, data sharing can endanger data theft.

4. Layer of software

The main issues in the IoT system are software concerns. To kill the system, viruses and assaults like a Trojan horse, worms, and malware, and so on are used to attack software that may violate data, modify information, corrupt IoT device systems, and access useful information.

- **Phishing Attack**

The opponent can collect relevant information and access personal information in this kind of attack by creating user authentication. These attacks have been used to steal passwords, credit card details, and so on.

- **Virus, Malware, and Spyware**

The attacker has IoT with malicious software that has varied effects. Such attacks damage the system by denying its functions, changing the information, and accessing private data.

- **Scripts Malicious**

In IoT, devices are frequently connected and communicated over the Internet. The system occurs to a complete shutdown when the user monitors the gateway and runs the active-X script [10]. This form of programming is used for web-based applications to check access and data theft.

- **Data Protection and Recovery**

By injecting the denial of service from the IoT network via application layers, the opponent can influence all users on an IoT system network so unauthorized users may access the system information. The attack type also prevents licensed users from connecting to the layer of the application. The attacker might have complete layer access to the application.

- **Denial Service**

Data communication involves user privacy. Personal information may be lost or even damaged by poor processing and data processing algorithms. DDoS attacks are normally launched in a coordinated manner from multiple attackers at the same time, and their detection before the services become unavailable is quite difficult [15]. The destructive impacts of IoT applications denial of service (DoS) attacks are being achieved. IoT services and devices are key aspects of IoT applications. DoS attacks damage IoT systems and disturb their usual operations.

B. Measures of Security Attacks in IoT

Measures of the mentioned attacks are detailed in this section.

1. Physical Layer Security

The lowest IoT network layer is the physical layer offers various hardware security measures.

- **Physical Secure Design**

The development of physically safe technologies is responsible for most hazards in the physical layer. The design of components such as acquisition units, radio frequency circuits, and so on should not modifiable and not of high quality. In WSN the design of the antenna is physically secure and has the ability to communicate over long distances [10].

- **Authentication of the Device**

If a new physical device enters the IoT network, the device should verify itself before sending and receiving the data. The technology keeps harmful devices out of the network if the device is correctly recognized.

- **Booting Safe**

The authenticity and originality of the software can be checked by applying a cryptographic hash algorithm [10]. This method monitors the digital signature for device software. Many hash algorithms cannot be implemented due to the weak processing skills of different devices.

- **Data Confidentiality**

All tags and data on each physical device must be confidential before secret information is delivered. The strong technique of cryptographic encryption such as AES cannot be applied because power consumption is low [10].

- **Privacy of Data**

Symmetric and asymmetric encryption functions like DSA, RSA, BLOWFISH, and DES, etc. guaranteed data privacy by preventing the attacker from unauthorized access of essential data when data is sending to the destination [10]. Due to their decreased power consumption, these encryption algorithms are easy to employ.

2. Network Layer Security

Several kinds of assaults challenge the network layer. Due to multiple wireless channels are seen, the attacker can alter device-to-device connectivity.

- **Privacy of Data**

The security control system monitors the network for any

kind of errors and uses the integrity of the data to explain the comparability of the received data with the original, such as point-to-point encryption. Authentication is unlawful sensor node access to data is utilized to prevent it.

- **Ad-hoc Safety Route**

Security aware ad hoc routing (SAR) protocol prevents inside attacks of the network of IoT [10]. The packets are added to certain security measures, and following analyses of received data, the opponent has been dropped out of the network.

- **Authentication**

Unlawful node access can be avoided using the correct authentication and encryption techniques. The most prevalent sort of assault in a DoS attack is a network layer that can influence the network through excessive information.

- **Routing Safety**

Safe routing is important for the sensor of a network in many applications. Due to the insecure routing protocols, different routing algorithms are applied to secure the confidentiality of data transferring towards various sensor nodes in IoT systems [10]. Therefore, many pathways ensure safe routing which fixes network faults and enhances the system's speed. Source routing is a technique used for the routing of sent data in packets following examination of data it is then transferred for processing.

- **System for GPS Position**

The GPS has experienced a network IoT system spoofing attack. The GPS locating technology, which is still the best possible option, was described and implemented.

3. Processing Layer Security

In the processor layer, several security measures are explored.

- **Web Application Scanners**

This program is used to identify various risks that are at the front of the web. Other web firewall software also identifies possible attackers.

- **Redundancy Dispersion Fragmentation**

In FRS the essential data onto the cloud is split and allocates to

various fragments of storage in servers [10]. No valuable data information that minimizes the risk of data theft is included in the fragment.

- **Encryption Homomorphic**

This is based on the entire process of homomorphic coding. This cypher text may be calculated without decryption instantly. Strong data security calculations are needed for this strategy.

- **Encryption**

Encryption technology is utilized to maintain IoT data confidentiality. Data will be encrypted first and transferred to the cloud afterward. Encryption helps against assaults on the side channel. There are various kinds of encryption such as Advanced Encryption Standard [10].

- **Safe Hyper**

Hyper safe protects the memory pages from being modified and limits the pointer index to modifying controlled data in pointer indexes.

4. Application Layer Security

The following is the category of security measures in the layer of an application.

- **Data Security**

Authentication and integrity are the key steps to ensure data confidentiality and IoT system encryption's whole privacy at this level. It prevents unwanted data access and protects hacking or theft of data.

- **Detection of Intrusion**

The intrusion detection process provides security solutions to many threats by producing an alarm when any uncertain action is performed in the system because of continuously controlling a log of intruder's activity [10]. Different detect approaches such as data mining abnormal detection can lead to intrusion detection.

- **Risk Assessment**

The risk evaluation generates effective safety measures and improves existing designs and safety planning.

- **The Firewalls**

When encryption, authentication, and ACLs process failed to block the unauthorized user then a firewall comes in process for the blockage [10]. The encoding and authentication procedure might be failed when selecting a low password. Filtering packets in the firewall is done thus, unwanted packages blocking.

- **Anti-Viruses, Spyware, and Adware**

For the IoT network's confidentiality, dependability, and integrity, software that offers anti-virus, anti-spyware and anti-adware security is required.

III. IoT Applications

Any future IoT solutions that take account of technological growth and the complex needs of potential customers cannot be envisaged. These requests detail these implementations as well as the scientific challenges. The adoption of IoT in manufacturing enables the transition of traditional manufacturing systems into modern digitalized ones, generating significant economic opportunities through industries re-shaping [19]. IoT enables modern businesses to take in innovative data-powered approaches to address global competitive pressure more efficiently. More and more gadgets are equipped with sensors, manufacturing tools, facilities, vehicles, and production equipment.

A. Intelligent Cities

Now we can see that many cities developed and city networks, branded and incorporated. With more than 60 percent of the world population expected to live in urban cities by 2025, urbanization as a trend will have diverging impacts and influences on future personal lives and mobility [18]. The rapid expansion of the town limits, fuelled by population growth and construction of infrastructure, will cause town borders to spread outward and swallow mega-cities into neighbouring cities. This will lead to the evolution of smart cities with eight smart features, including Smart Economy,

Smart Buildings, Smart Mobility, Smart Energy, Smart Information Communication and Technology, Smart Planning, Smart Citizen, and Smart Governance [18]. For the implementation of IoT the position of city councils is crucial. The use of the IoT would be guided by the execution of daily city activities and the establishment of a city planning strategy. Cities and their utilities, therefore, provide an almost perfect forum for IoT research considering city requirements and converting them to IoT-enabled solutions. The smart city embraces several areas that involve innovative technologies, and one important area is communal sharing [17].

B. Intelligent Energy and Intelligent Grid

This will help to raise awareness of our changing electricity, consumption, and infrastructure policy paradigms. Our electricity supplies in the future can no longer be dependent on fossil fuels for many reasons. Nuclear power is still no future-proof choice. Therefore, potential electricity supplies can primarily be dependent on different renewable resources. Our energy usage behaviour must be increasingly focused. Because of its volatile nature, such supply demands an intelligent and flexible electrical grid that can react to power fluctuations by controlling electrical energy sources (generation, storage) and sinks (load, storage) and by suitable reconfiguration [18]. These features are largely based on IoT standards for networked intelligent systems like devices, micro-generation devices, infrastructures, consumer products, and components of grid networks. This ideal includes an understanding of the instantaneous energy consumption of different charges, such as equipment, machinery, and manufacturing equipment, to notify each consumer of its energy use.

C. Intelligent Mobility and Transport

Vehicle access to the Internet creates a range of new options and technologies, which make travel faster and more secure for individuals. In this context, the

concept of Internet of Vehicles (IoV) connected with the concept of Internet of Energy (IoE) represents future trends for smart transportation and mobility applications [18]. Focusing on confidence, safety, and simplicity in mobile networks or contactless transit applications, at the same time would make purchases or customer services safer, accessible, and convenient. It is a challenge to represent human behaviour when designing, developing, and operating cyber-physical structures on independent vehicles. Including human aspects is essential for safety, predictability, and reliability. There is little knowledge of the impact of cyber-physical driver behaviour's adaptive traffic control systems. As cyber-physical systems become more complex and interactions between components increases, safety and security will continue to be of paramount importance [18].

D. Medical Devices IoT

IoT devices are also commonly employed to monitor and analyze patients in healthcare systems. To monitor the medical condition of a patient, Personal Medical Devices (PMDs) are either planted in the patient's body or may attach to the patient's body externally [20]. The market value of these devices is projected to be around 17 billion dollars by 2019 [20]. These devices are connected to a base station through a wireless interface, which is further utilized for reading the device status, medical reporting, and change device parameters, or updating device status. The wireless interface poses several hazards to the patient's security and privacy. Cyber-attacked gadgets are extremely easily available over the wireless interface, which might endanger patients' safety, privacy, and security. In the case of health care, the primary goal is to ensure the security of the network to prevent the privacy of patients from malicious attacks [20]. Mobile devices have predefined targets when attacked. The objective is generally to rob information, attack resources, or discontinue specific programs which

monitor the patients' status.

E. IoT Intelligent Home

The IoT smart home services are increasing day by day, digital devices can effectively communicate with each other using Internet Protocol (IP) addresses [20]. The increasing amount of equipment also enhances malicious assault in the intelligent home environment. If smart home equipment runs alone, malicious threats are decreased as well. Currently, intelligent domestic on the internet everywhere, gadgets may be accessed. It thereby raises the risk of these devices being attacked maliciously. A smart house has four components which are a service platform, a smart device, a home portal, and a home network. Many gadgets are connected to the intelligent home and intelligently distribute information across the home network. Therefore, a home portal is available to monitor data flow between intelligent devices linked to the external network. The Service Platform utilizes the Service Provider services providing diverse home network services. Mobile devices simultaneously guarantee that customers have access to the gadgets linked to the network to a portable "controller". Many enterprises explore building platforms integrated with health supervision, energy monitoring, and the monitoring of wireless sensors in homes and buildings.

IV. Conclusion

This article focused mostly on security challenges for IoT, concentrating on security threats and their actions. As IoT devices lack security mechanisms, a lot of IoT devices have become soft goals, and the victim does not know they are compromised. The security needs of confidentiality, integrity, and authentication are explained here, and so on. Given the security relevance for IoT applications, IoT devices and communication networks must incorporate security mechanisms. It is also recommended that you do not use basic device passwords and understand device protection needs before first utilizing them to prevent intruder or security

concerns. Disabling unused features may reduce the likelihood of security threats. Moreover, many security methods utilized in IoT devices and networks are vital to examine.

V. Acknowledgment

The authors would like to thank all School of Computing members who were involved in this study. This study was conducted for the System and Network Security Research Project. This work was supported by the Ministry of Higher Education Malaysia and University Utara Malaysia.

VI. References

[1] Perwej, Y., Haq, K., Parwej, F., Mumdouh, M., & Hassan, M., "The Internet of Things (IoT) and Its Application Domains," *International Journal of Computer Applications*, 975(8887), pp. 182, 2019.

[2] Rao, T. A., & Haq, E. U., "Security challenges facing IoT layers and its protective measures," *International Journal of Computer Applications*, 179(27), pp. 31-35, 2018.

[3] Prasad, R. R., & Damle, P., "Personalization And Privacy In Iot: A Consumer-Business Challenge," *PalArch's Journal of Archaeology of Egypt/Egyptology*, 17(6), pp. 4554-4567, 2020.

[4] Hussein, D. M. E. D. M., Hamed, M., & Eldeen, N., "A blockchain technology evolution between business process management (BPM) and Internet-of-Things (IoT)," *Int. J. Adv. Comput. Sci. Appl*, 9(8), pp. 442-450, 2018.

[5] Klein, A., Pacheco, F. B., & Righi, R. D. R., "Internet of things-based products/services: process and challenges on developing the business models," *JISTEM-Journal of Information Systems and Technology Management*, 14(3), pp. 439-461, 2017.

[6] Alkhalil, A., & Ramadan, R. A., "IoT data provenance implementation challenges," *Procedia Computer Science*, 109, pp. 1134-1139, 2017.

[7] Bujari, A., Furini, M., Mandreoli, F., Martoglia, R., Montangero, M., & Ronzani, D., "Standards, security and business models: key challenges for the IoT scenario," *Mobile Networks and Applications*, 23(1), pp. 147-154, 2018.

[8] Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B., & Ande, R., "IoT standardisation: Challenges, perspectives and solution," *In Proceedings Of The 2nd International Conference On Future Networks And Distributed Systems*, pp. 1-9, 2018.

[9] Lee, I., "The Internet of Things for enterprises: An ecosystem,

architecture, and IoT service business model," *Internet of Things*, 7, 100078, 2019.

[10] Ahmed, A. W., Ahmed, M. M., Khan, O. A., & Shah, M. A. A, "Comprehensive analysis on the security threats and their countermeasures of IoT," *International Journal of Advanced Computer Science and Applications*, 8(7), pp. 489-501, 2017.

[11] Hwang, Y. H., "Iot security & privacy: threats and challenges," *In Proceedings of the 1st ACM workshop on IoT privacy, trust, and security*, pp. 1-1, April 2015.

[12] Johnson, D., & Ketel, M., "IoT: Application Protocols and Security," *International Journal of Computer Network & Information Security*, 11(4), 2019.

[13] Nebbione, G., & Calzarossa, M. C., "Security of IoT application layer protocols: Challenges and findings," *Future Internet*, 12(3), pp. 55, 2020.

[14] Lee, I., & Lee, K., "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Business Horizons*, 58(4), pp. 431-440, 2015.

[15] Hameed, S., Khan, F. I., & Hameed, B., "Understanding security requirements and challenges in Internet of Things (IoT): A review," *Journal of Computer Networks and Communications*, 2019.

[16] Rane, S. B., & Narvel, Y. A. M., "Re-designing the business organization using disruptive innovations based on blockchain-IoT integrated architecture for improving agility in future Industry 4.0," *Benchmarking: An International Journal*, 2019.

[17] Viriyasitavat, W., Anuphaptrirong, T., & Hoonsopon, D., "When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities," *Journal Of Industrial Information Integration*, 15, pp. 21-28, 2019.

[18] Fantana, N. L., Riedel, T., Schlick, J., Ferber, S., Hupp, J., Miles, Svensson, S., "IoT applications–value creation for industry," *Internet Of Things: Converging Technologies For Smart Environments And Integrated Ecosystems*, pp. 153, 2013.

[19] Mourtzis, D., Vlachou, E., & Milas, N. J. P. C., "Industrial big data as a result of IoT adoption in manufacturing," *Procedia Cirp*, 55, pp. 290-295, 2016.

[20] Razzaq, M. A., Gill, S. H., Qureshi, M. A., & Ullah, S., "Security issues in the Internet of Things (IoT): A Comprehensive Study," *International Journal of Advanced Computer Science and Applications*, 8(6), pp. 383, 2017.