Grenze International Journal of Engineering and Technology, Jan Issue

Challenges to IoT Security: Industry Perspective

Manju Lata[1] and Vikas Kumar[2]
[1]Chaudhary BansiLal University, Bhiwani – 127021, Haryana, India
Email: manjulata94@gmail.com,
[2]Central University of Haryana, Mahendergarh - 123031, Haryana, India
Email: prof.vikaskumar@gmail.com

***Abstract*—The increasing adoption of Internet of Things (IoT) technologies and their related applications give rise to extensive challenges due to integration of varied categories of devices and technologies. Predominantly, this offers major challenges to the large number of industries to creates and run security policies that cover all functional areas. Currently, high-tech standards used for particular IoT security in the perspective of industry are simply the beginning of addressing by established IT security standards groups, associations, and vendor associations. It is also difficult for most government bodies and regulatory bodies to develop worldwide recognized security standards. Present work identifies the different challenges and opportunities concerning security issues in the IoT. An overview of effective IoT-related cases on major challenges accepted by the industry was presented. At the same time, the major opportunities that the industry can work with are also presented.**

***Index Terms*— Internet of Things (IoT), IoT Security, High-tech Standards, Challenges and Opportunities.**

I. INTRODUCTION

The emerging trend of technology is continuously changing people's lives. In addition to some of these emerging technologies, the IoT has been recognized as a machine-to-machine (M2M) technology where smart devices connect data, process information, organize and communicate information to the whole world, and perform actions dynamically or robotically [1]. The IoT is a new standard that relies on the interplay of smart devices with inter alia of physical or virtual resources via the Internet. IoT is a system connecting people and machines, gathering together services, environment, context and intellectualizing process [2]. IoT has developed not only through a wide variety of underlying technologies but also from side-to-side developments in different fields, each with vastly dissimilar purposes. In addition, IoT developments have been organized in different application areas that regularly use specific and exclusive standards [3]. Up-and-coming IoT applications can make many things in business as well as human life easier and lead to a smarter world. This is a sign of development that can bring intense changes in the world of business. During a technology-driven revolution that is changing business and the world, Artificial Intelligence (AI), automation as well as a digital invention are enabling devices to attach and absorb at an unexpected scale [3].

According to IDC (2022) predictions, 50% of innovative operational assets became self-sustain and $14.3 billion of services were consumed to make IoT resolutions in 2020 (https://www.idc.com/itexecutive/research/topics/iot). In 2022, industry environments identify 40% more development ratio of innovative digital and physical products and services carried to market in contrast to old-

Grenze ID: 01.GIJET.9.1.707

style revolution methods [4]. Furthermore, The IoT technology market is estimated to grow from USD 384.5 billion in 2021 to USD 566.4 billion by 2027 at a CAGR of 6.7% [5]. Even though the worldwide IoT market size grew by 22% in 2021, the worldwide enterprise IoT market grew by 22.4% to reach USD 157.9 billion in 2021 [6]. The market grew somewhat slower than expected by 24% last year because of quite a few issues, containing a slower-than-expected total economic recovery, costly or unavailability of chipsets, and interrupted supply chains. North America became a rapidly increasing zone in 2021 with +24.1%, and process manufacturing was the fastest increasing segment with +25%. Right now, IoT Analytics predicts that the IoT market size grow by 22.0% to $525 billion at a CAGR from 2022 to 2027. The five-year prediction has been reduced from the past year [6]. Quite a lot of headwinds to growth have had a much deeper impact than earlier expected, especially supply shortages and interruptions (mainly chip shortages estimated up to 2024 and perhaps further than) and lack of labour, particularly in exclusive software trades. Regardless of reduced growth forecasts, IoT rests on a very high-class technology, with lots of projects towards the inside deployment stage. The worldwide several connected IoT devices are estimated to reach 14.5 billion by the end of 2022 [6].
IoT is growing exponentially, but securing IoT projects and services remain a lot challenge from the industry perspective. One of the most essential security aspects of the IoT is to ensure that devices and services have trustworthy identities, and that can interrelate with secure environments. Some of the security-related aspects associated with IoT include the complexity of establishing safe and secure communication [7]. Regardless of this, IoT requires some security standards and use cases are very much vital for meeting the challenges at a worldwide level [3]. Some vulnerabilities can lead to system failure or a hacker attack, which can disturb people. For example, traffic lights can stop working and cause traffic accidents; or the household security system can be turned off via thieves. As some IoT devices are used for industry, automation, smart warehouse, healthcare or social protection, their security can be serious to people's lives [8].

II. Security Challenges

In 2021, there were 1.51 billion breaches of IoT devices, however, in 2020, Kaspersky stated 639 million breaches [9]. Underrating the significance of cyber security in the growth of IoT systems is improper [9]. IoT-aided devices pose more than a few security challenges for their consumers. Even though IoT has carried incredible connectivity on behalf of devices, the shared IoT security problems are not changed. In addition, there are also several dangerous threats of IoT, for example, insignificant computing power, sharing of network access, unpredictable security standards, lack of firmware updates, and more. To identify how to secure IoT systems, it is crucial to early examine the possible IoT cyber security challenges, for example, Software and firmware vulnerabilities, insurance communications, data leaks from IoT systems, malware risks, and cyberattacks [10,11]. There are some biggest security challenges concerning the field of IoT-connected devices.

A. Lack of proper testing and updates

One of the foremost difficulties tech industries have in creating these devices is being too careless when it comes to controlling the security risks associated with the devices. Many of these IoT devices as well as products do not receive sufficient updates, even though some do not receive critical security updates of any kind [11]. Its means the device that was once considered secure when clients first purchased it comes to be insecure and ultimately vulnerable to hackers and other security issues. Primary computer systems had a similar difficulty that was slightly resolved by automatic updates. Conversely, IoT makers are more excited to manufacture and offer the devices as quickly as they can devoid of worrying excessively about security. Inappropriately, best manufacturers only provide firmware updates for a slight time, merely to stop when they start functioning on the next interesting gadget. Even poorer, they procedure unproven older Linux kernels. Their trusted clients are thus unprotected from possible attacks due to obsolete hardware and software.

B. Brute enforcement and the problem of defaulting passwords

The Mirai botnet, applied in some of the major and utmost destructive DDoS attacks, may be one of the greatest examples of the issues derived from using shipping devices and using default passwords besides not stating users to alter them once they collect them. Approximately government indicators instructing creators not to sell IoT devices using poor security login details, for example, use of admin with username as well as password. This means that they are now nothing over the advice and there are no legitimate consequences to motivate creators to unrestraint this risky use. Weak passwords and credentials make almost entire IoT devices at risk of password hacking as well as especially brute force. The single intention of Mirai malware became so effective because it recognized at-risk IoT devices and usage of default passwords to log in to infect. Consequently, any industry that

has used defaulting login on the devices is putting their industry, resources as well as clients in addition to their important information vulnerable to being subjected to a brute force attack [12].

C. IoT malware and ransomware

As lots of IoT devices constantly grow in the coming stage of development, same will the several malware and ransomware utilized to exploit them. Whereas traditional ransomware depends on encryption to absolutely lock out consumers from diverse devices as well as platforms, there is continuing hybridization mutually of malware as well as ransomware that targets to join dissimilar attacks. Ransomware attacks may perhaps target to limit and/or deactivate device serviceability while stealing user data. Such as, the modest IP camera is perfect for capturing sensitive data in an inclusive variety of locations, including households, workplaces, or even native gas stations. Then webcam can be locked and directed to an infected web address, which may perhaps obtain sensitive data with a malware entrée point and request a ransom to unlock the device in addition to returning the data [13]. The forever developing IoT devices will create randomness in the future when it comes to illegal access or theft.

D. IoT botnets targeting cryptocurrencies

The intense mining competitiveness along with the cutting-edge growth in cryptocurrency estimations is evidencing too tempting for hackers looking to trade in on the crypto-craze. Even though furthermost consider blockchain to be hacker-proof, quite a lot of attacks in the blockchain area look to be on the rise. The foremost weakness is not the blockchain itself, but somewhat the growth of the blockchain application that runs on it. Social engineering is before now utilized to obtain usernames, passwords as well as private keys, in addition, it will be utilized more frequently to hack blockchain-based applications in the future. The open-source cryptocurrency Monero is the only of the several digital currencies presently being mined using IoT devices [14]. Quite a few hackers have even redesigned IPs as well as video cameras for cryptocurrency mining. IoT botnet miners, Blockchain breaches, as well as data reliability manipulation mien an enormous threat to flood the open crypto market as well as disturb the previously unstable value and configuration of cryptocurrencies.

E. Data privacy and security across phone, web, and cloud

Data protection and security remain to be one of the biggest challenges in nowadays' connected globe. Data is continually being used, pass on, warehoused and deal with the huge industries via varied IoT devices, for example, smart televisions, smart lighting systems, attached smart printers, smart HVAC systems, smart sensors and thermostats. Usually, entirely the customer data is distributed or even retailed to several industries, which violates the civil liberties to privacy and data protection and increases personal doubt. Insufficient data protection is also a risky IoT security concern. This problem can happen due to unsafe data storage and uncertain communication. One substantial vulnerability in IoT security is becoming the negotiated device that can be utilized to access confidential data [15]. The significance of protected data storage as well as web-based network isolation has never been clearer.

F. AI and Automation

As IoT devices continuously attack daily life, industries will ultimately have to manage quite a lots of IoT devices. This quantity of consumer data can be problematic to deal with in terms of data assembly and networking. AI and automation techniques are now being utilized to filter huge quantities of data and can support IoT managers as well as network security professionals to apply data particular procedures and identify irregular data and traffic configurations. Though autonomous systems create autonomous decisions that interrupt the number of roles across huge infrastructures, for example, energy, healthcare, and shipping can be more dangerous, specifically when you realize that a single code error or incorrect algorithm can cause the crash whole infrastructure.

G. Security issues in managing device updates

Software and firmware be able to one of the biggest causes that can interrupt software security. But, the creator can provide modern product updates using devices it retails. These updates may likely cause security breaches.
These are some of the utmost persistent IoT security challenges that became essential to consider while manufacturing IoT-based applications in the coming years. Most of them rotate around two things, securing IoT in contrast to attacks and securing user data contrary to theft.

III. Cases on Major Challenges

In the world of users and enterprises, IoT has continued growth and enhanced inventions, however, IoT security breaches are also on growth. Connected smart devices are all over the place and have taken root in our individual and proficient networks. From automatic security systems to sensors that can be set from portable devices, and from voice-activated peripherals that enable the less able to live independently, to pioneering inventions, for example, self-driving cars. Though, with over 26.66 billion active IoT devices in 2020 and estimated to develop to 75 billion by 2025, the IoT is not devoid of risks [16]. Sensitive data, cloud technologies, also vast numbers of smart devices are attached through the Internet, offering cyber criminals a huge attack superficial. 84% of measured industries described IoT security breaches [16]. Inappropriately, several IoT devices are not prepared to be secure by default while they ship from creators, also because of their frequently embedded nature, they are not often patched as well as protected once in manufacture. Any network weaknesses can simply exploit by hackers as well as under attack through malware. Enterprises must therefore make sure that they have strong security with compliance management prepared for all IoT touchpoints. There are some actual examples of IoT security breach cases that have happened in the IoT in the past.

A. Apple listened to conversations without any consent

Before this year, Apple's so-called 'Facepalm' bug hit the headings. It happened in Arizona when a 14-year-old boy was joining his friend in a group conversation [17]. Even though the friend never attended to the phone, the boy was able to hear in on the conversations arranged on the friend's iPhone, as per ZDNet. Despite the boy's limitless efforts to inform the case to Apple, Apple did not take action until a week after the incident happened. Consequently, Apple decided on a security flaw extremely and announced the software update that would later fix the bug [16].

B. WiFi router unprotected to malicious code

Also happened before this year, the utmost standard WiFi chipsets (Marvel Avastar 88W8897 firmware) on the marketplace were unprotected to the weakness that could be activated devoid of any user interface, as per ZDNet [17]. It is installed on devices with PlayStation 4, Xbox One, MS Surface Laptops, Samsung Chromebooks and smartphones. Conversely, it was determined to be solely an issue with the app's firmware, and fixes were issued after the occurrence [16].

C. IoT device infected with this malware

In 2017 as per Larry Cashdollar, one of Akamai's scholars, encouraged via the old BrickerBot strain, Silex Malware functioned by destroying IoT device storage, invalidating firewall procedures, eliminating the configuration of the network, as well as stopping devices. The malware rapidly spread among IoT devices, causing 1,650 attacking devices [17]. Intending to improve, vendors had to automatically reinstall the firmware of all devices. Amazingly, this malware was spread through the 14-year-old teenager with the pseudonym Light Leafeon [16].

D. ID can leak or chances of ID leaked

Before this year, a bug in the Bluetooth communication protocol affected users of up-to-date devices to be tracked and their ID leaked, as per ZDNet in 2019 [17]. It may be applied to spy on customers regardless of the instinctive securities the operating system (OS) had and could affect the devices of Windows 10, iOS and macOS. Though, as stated by Boston University's search, this algorithm does not include message decryption, nor does it compromise Bluetooth security at all [16]. Microsoft (MS) also publically declared that the problem was fixed in the May 2019 update.

E. Alexa and Google Home devices are eavesdropping on users over again

In addition to many outcomes in 2018, hackers once again misused Alexa and Google Home smart aides to eavesdrop on users devoid of their information, or worse, trick consumers into giving over sensitive data, as per ZDNet [17]. No problem that how Amazon and Google have installed updates consistently, innovative ways to abuse the device seem to keep popping up.

F. Hackable Cardiac devices

In 2017, CNN defined, The FDA showed that St. Jude Scientific's embeddable cardiac devices have weaknesses that can permit a hacker to get entry to a device. the FDA stated that just once, they may expend the battery or administer improper pacing or tremors. While pacemaker devices and defibrillator devices became utilized to

monitor and manipulate patients' coronary heart functions and prevent heart assaults [18]. The item persisted to describe the vulnerability happened within the transmitter that delivers the devices' information and remotely shares it with physicians. The FDA stated that hackers can control a device by using getting access to its transmitter.

G. Mirai Botnet (DDoS attack)

In October of 2016, the biggest DDoS attack constantly released on service supplier Dyn the usage of IoT botnet [18]. This causes massive portions of the internet to take place, consisting of Twitter, the Guardian, Netflix, Reddit, and CNN. This IoT botnet was prepared by malware named Mirai. When crumbling or transmissible through Mirai, computer systems always seek the internet on behalf of weak and at-risk IoT devices after which use regarded default usernames and passwords to credential as well log in, spoiling them through malware. these gadgets were equipment similar to digital cameras and DVR players.

H. The Jeep Hack

The IBM protection Intelligence website informed us about the Jeep hack. In July 2015, a group of scholars became capable of takings the total operation of a Jeep SUV with the use of the automobile CAN bus [18]. As a result of developing a firmware replacement vulnerability, they hijacked the automobile over the sprint cellular network and found they may make it go faster, secure down, or even veer off the path. Its impervious conception on behalf of the increasing IoT hacks: while industries frequently overlook the protection of peripheral devices or networks, the significance may be tragic.

With IoT devices as well as technologies, evolving so rapidly risks and attacks become a flawless, and existent vulnerabilities to users and enterprises around the globe. Consequently, users must identify how to secure their information and devices from this misuse. Users should take this enormously and understand that disappointments can have tragic consequences. Paying attention to personal information will also permit creators and industries to emphasize more the prime goals of IoT that developing the industries, quality of life cycle as well as user capability. Furthermore, there is essential to develop the greatest security standards, protocols and approaches if the IoT uprising is to sustain to distribute importance to human beings devoid of giving up protection.

IV. OPPORTUNITIES

The IoT is at the peak of development through wireless and sensing connectivity, in addition to aid specified via processing, control and power management devices in existing years [19]. The phase is now established on behalf of the IoT to initiate sighted by standard deployment together with users and industry domains. There are subsequently described the challenging situations and opportunities of IoT from the perspective of the industry. Extremely unified solutions to support take hold of the enormous business-related opportunities [20,21].

A. Industry specialist firm market and markets approximations by 2022 the wide-reaching IIoT enterprise may be real assets about $195 billion yearly. Estimates about the several attached IoT devices to be in process differ quite substantially. Furthermost determined that there might be 50 billion in 2020, whereas others claim 20 to 30 billion is more sensible. Progressively, there will be tens of billions of things connected to the internet in support of coming years, in addition about 50% of these might be on behalf of industrial utility (https://www.arrow.com/en/research-and-events/articles/challenges-and-opportunities-of-industrial-iot-technology).

B. Industrial IoT can allow better automation and for this reason, increase productiveness. It can additionally help organizations to increase the collection of services they may provide, enhance security, keep away from interruption, recover and control the resources as well as turn out to be greater environmentally liable.

C. There is the majority of various associated technologies provided with a purpose to aid industrial IoT. Approximately few of these are now established, whilst others are quite the procedure of rising. They encompass conventional business wireline protocols (for example CAN bus, Fieldbus, Hart, KNX, Ethernet, MBUS and PLC), in addition to Wi-Fi protocols. The Wi-Fi wireless connectivity alternatives may be classified as both mobile-based ones that keep the extensive area network (such as LTE−M, and 5G) or quick-range, energy-efficient ones (such as Wi-Fi®, LoRa, ZigBee®, Z-Wave® and BLE) on behalf of the continuing implementation.

D. IoT provides an opportunity to manage distinctive devices remotely through cloud-based automation setups, such as stimulating lighting, using vehicles, beginning/ending actions, and many others. Li-Fi communication is allowing the capability to know about formerly traditional standalone actuators. Similarly, dissimilar sensor

technology can be engaged in an industrial IoT environment, including the temperature at which the commercial manner is being carried out, energy consumption as well as capacity load throughout the utensils process, the ambient light as well as dampness tiers in a huge business greenhouse, or nitrogen-oxide contented material in the air leaving the use flu of business container.

E. On behalf of sensor-related networks, the energy consumption of the things is in all likelihood to be considerably less than may be the case for related actuators; as a result, battery-powered things will constitute the sizeable substance of deployments. this is probable to demonstrate energy to IoT propagation, as several apps will depend on sensors that have been organized in remote locations. The energy consumption and linking range of the radio interface will possibly constitute a good-sized effect on the duration of the battery (thus BLE and ultra-low power RF protocols are most effective).

F. Along with the constraints engaged on industrial-based IoT hardware because of battery-powered procedure, the microchip technology located at each node is probably to have other restrictions. The wide range of devices deployed ought to mean that small bill-of-substances prices want to be observed too. moreover, to be had space will also be constrained.

G. The cloud can be the consideration upon which IoT information processing and storage actions are dependent. Industrial IoT-based records need to be controlled below very strict deployment procedures as well as authorization of the holder of these facts. To moderate the possible hazard of industrial undercover activities, hacking or even deeds of violence, a completely protected supplier provides requirements to be hired.

H. ON Semiconductor standard renowned in advance that somewhat becomes had to be carried out about the disjointed form that occurs in the middle of the hardware and software components of IoT improvement. In the end outcome of this enterprise turned into the ON Semiconductor IoT development kit (IDK). This affords engineers using a solitary platform that recognized an extraordinary elasticity, upon which the needs of both hardware and software programs are embarked. Depending on the industry's vastly fashionable NCS36510 system-on-chip (SoC) through 32-bit ARM® Cortex® M3 processor core, it contains the important hardware sources behalf of making surprisingly powerful, distinguished industrial IoT devices, at the side of a wide-ranging software context appear to interface using the cloud [22].

I. with the aid of assigning daughter cards to the IDK baseboard, a means of conferring (WI-FI, SIGFOX, Ethernet, 802.15.4 MAC-based radios permitting ZigBee and Thread protocols, and so on.), and sensor (motion, ambient light, proximity, heart rate, and so on.) and actuator (using stepper and brushless motor using, plus the capacity to force LED strings) possibilities may be brought to the machine [23].

J. The Eclipse-based connected development environment (IDE) attends the hardware including a C++ code editor, compiler, and debugger with the group of software-associated libraries. It permits them to organize the IDK in the manner that pleasant suits with software, while concurrently quite advancing commencing effective security functions and actual-time diagnostics/analytics. The IDK gives an extraordinary platform to assist engineers to reap their gadget layout desires at the same time as accelerating development timeframes, thus deploying systems earlier using price efficiency.

V. Conclusion

Industries can attain massive benefits from developing IoT-based devices and applications, but their security is one of the main issues. This paper covered all about IoT security and how to overcome it. Governments despite the business or increasing size can create IoT resolutions as a part of their industry to develop user satisfaction and efficiency. This paper also provides an overview of the opportunities afforded by the huge technology, concerning machine to machine, users to their surroundings and enables exploration of the globe on the innovative aspect. While opportunities become substantial and go together with the risks for the company and its setup. This paper covered some crucial points related to challenges and opportunities concerning the security issues in IoT perspective of the industry.

Reference

[1] AboBakr, & M. A. Azer, "IoT Ethics Challenges and Legal Issues", In *2017 12th International Conference on Computer Engineering and Systems (ICCES)*, pp. 233-237, IEEE, December 2017,

[2] Bojanova, G. Hurlburt, & J. Voas, "Imagineering an internet of anything", *Computer*, vol. 47, No. 6, pp. 72-77, 2014, doi:10.1109/MC.2014.150

[3] M. Lata, & V. Kumar, "Standards and Regulatory Compliances for IoT Security", *International Journal of Service Science, Management, Engineering, and Technology (IJSSMET)*, vol. 12, No. 5, pp. 133-147, 2021.

[4] Hojlo, A. Pinder, M. Dialani, C. Holmes, K. Ko Shikita, L. Veronesi, "IDC Future Scape: Worldwide Manufacturing Product and Service Innovation 2021 Predictions", 2020, [Available at]: https://www.idc.com/research/viewtoc.jsp?containerId=US46915020
[5] Markets and Markets, "IoT Technology Market by Node Component (Sensor, Memory Device, Connectivity IC), Solution (Remote Monitoring, Data Management), Platform, Service, End-use Application, Geography (2021-2027)", 2022, [Available at]: https://www.marketsandmarkets.com/Market-Reports/iot-application-technology-market-258239167.html
[6] P. Wegner, "Global IoT market size grew 22% in 2021 — these 16 factors affect the growth trajectory to 2027", 2022, [Available at]: https://iot-analytics.com/iot-market-size
[7] N. Alhalafi, & P. Veeraraghavan, "Privacy and Security Challenges and Solutions in IOT: A review", *IOP Conference Series. Earth and Environmental Science*, vol. 322, No. 1, 012013, August 2019, doi:10.1088/1755-1315/322/1/012013
[8] Lata, & V. Kumar, "IoT Network Security in Smart Homes", *Cybersecurity in Smart Homes: Architectures, Solutions and Technologies*, pp. 155-176, 2022.
[9] Cyrus, "IoT Cyberattacks Escalate in 2021, According to Kaspersky", 2021 [Available at]: https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/#:~:text=IoT%20cyberattacks%20more%20than%20doubled%20year-on-year%20during%20the,reported%2C%20an%20increase%20from%20639%20million%20in%202020.
[10] Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, & E. K. Markakis, "A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues", IEEE Communications Surveys & Tutorials, vol. 22, No. 2, pp. 1191-1221, 2020.
[11] H. F. Atlam, & G. B. Wills, "IoT security, privacy, safety and ethics", In *Digital twin technologies and smart cities*, pp. 123-149, 2020, Springer, Cham.
[12] Farik, & A. S. Ali, "Algorithm to Ensure and Enforce Brute-Force Attack-Resilient Password in Routers", *International Journal of Technology Enhancements and Emerging Engineering Research*, vol. 4, No. 10, pp. 184-188, 2015.
[13] Brierley, J. Pont, B. Arief, D. J. Barnes, & J. Hernandez-Castro, "PaperW8: an IoT bricking ransomware proof of concept", In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pp. 1-10, August 2020.
[14] R. Murimi, "Use of Botnets for mining cryptocurrencies", In *Botnets*, pp. 359-386, 2019, CRC Press.
[15] Y. Verginadis, A. Michalas, P. Gouvas, G. Schiefer, G. Hübsch, & I. Paraskakis, "Password: A holistic data privacy and security by design framework for cloud services", *Journal of Grid Computing*, vol. 15, No. 2, pp. 219-234, 2017.
[16] Jo. Vanwell, "IoT Security Breaches: 4 Real-World Examples", at Conosco, 2021, [Available at]: https://www.conosco.com/blog/iot-security-breaches-4-real-world-examples/
[17] Penta Security, "Top 5 Shocking IoT Security Breaches of 2019", 2019, [Available at]: https://www.pentasecurity.com/blog/top-5-shocking-iot-security-breaches-2019/
[18] T. Dunlap, "The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History", 2020 [Available at]: https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities
[19] K. K. R. Choo, S. Gritzalis, & J. H. Park, "Cryptographic solutions for industrial Internet-of-Things: Research challenges and opportunities", *IEEE Transactions on Industrial Informatics*, vol. 14, No. 8, pp. 3567-3569, 2018
[20] Sisinni, A. Saifullah, S. Han, U. Jennehag, & M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions", *IEEE transactions on industrial informatics*, vol. 14, No. 11, pp. 4724-4734, 2018.
[21] M. Serror, S. Hack, M. Henze, M. Schuba, & K. Wehrle, "Challenges and opportunities in securing the industrial internet of things", *IEEE Transactions on Industrial Informatics*, vol. 17, No. 5, pp. 2985-2996, 2020.
[22] R. J. Hassan, S. R. Zeebaree, S. Y. Ameen, S. F. Kak, M. A. Sadeeq, Z. S. Ageed, ... & A. A. Salih, "State of art survey for iot effects on smart city technology: challenges, opportunities, and solutions", *Asian Journal of Research in Computer Science*, *22*, pp. 32-48, 2021
[23] W. Voss, "Comparison Of CAN Bus And Ethernet Features For Automotive Networking Applications", 2019, [Available at]: https://copperhilltech.com/blog/comparison-of-can-bus-and-ethernet-features-for-automotive-networking-applications/