IRAQI Academic Scientific Journals

Al-Rafidain Engineering Journal (AREJ)   Vol.28, No.1, March 2023, pp. 312-320

Securing Industrial Internet of Things (Industrial IoT)- A Reviewof Challenges and Solutions

Mohammed B. Mahmood [*]
mohammed.enp95@student.uomosul.edu.iq

Jassim M. Abdul-Jabbar [**]
drjssm@almaaqal.edu.iq

[*] Computer Engineering Departement, Collage of Engineering, University of Mosul, Mosul, Iraq.
[**] Control and Computer Engineering Departement, Collage of Engineering, Almaaqal University, Basra, Iraq

Received: 2022-08-19   Received in revised form: 2022-09-27   Accepted: 2022-10-22

ABSTRACT

Industrial IoT (Industrial IoT) is a new promising technology which can be used to increase the amount of productions with high qualities. Industrial IoT technologies guarantee full control to the processes remotely through the internet which can reduce the number of workers in the field. As a result, this can reduce the percentage of worker injuries and accidents in addition to the total costs. The Industrial IoT systems are attractive targets to attackers. For this reason, these systems require high levels of security since such levels have direct effects on physical devices which may be dangerous on human life and safety. To guarantee high level of security, a combination between Information Technologies (IT) and Operation Technologies (OT) with new innovative methods should take place. In this paper, many new technologies and security methods are reviewed with their possible attacks in order to provide Industrial IoT infrastructure designers with the required information to take them into consideration. Also, differences and convergences between both classical Information Technology (IT) and operational Technology (OT) and their relations to the Industrial IoT systems are investigated with the possible attacks on each layer of the IT and the OT.

Keywords:

OPC UA ,Industrial IoT , Information Technology , operational Technology, SCADA, security threats.

https://rengj.mosuljournals.com

1. INTRODUCTION

The internet of things (IoT) applications are usually presented to connect devices through intelligent infrastructure. The term IoT has a variety of applications around the world, but if the applications are related to the manufacturing segments and industrial processes, then it is known as Industrial IoT (Industrial IoT). The Industrial IoT applications depend basically on industrial communication networks. Before the revolution of the Industrial IoT, there was no communication link between various industrial systems and they were not connected to the internet. Nowadays, industrial communication networks are highly dependent on open protocols and platforms. For this reason, the industrial communication networks are developing very fast, but at the same time the percentage of cyber-attacks on these systems are increasing too [1]. Fig. 1 shows a generalized Industrial IoT system architecture.

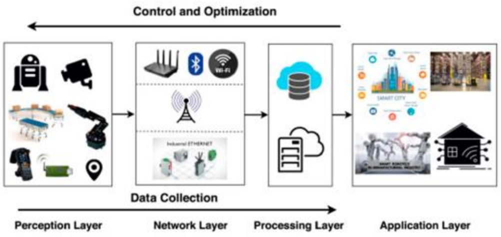

Fig. 1. Generalized Industrial IoT system architecture.

The Industrial IoT can also be called Industry 4.0 [2]. The term industrial communication is related to the data transfer between industrial equipment and devices by using special types of protocols for each industrial layer. There are three main industrial communication protocols: real-time Ethernet (RTE), Fieldbuses and wireless networks [3]. Recently, securing the Industrial IoT has become a distinguishable topic because of three reasons; firstly, there is a strong relationship between Industrial IoT and IT. Secondly, the traditional security methods of IT systems cannot be applied directly to the Industrial IoT information and finally, hackers, viruses and worms turn to be more and more powerful due to the advanced technologies in the field of software and microprocessors [4].

2. Related Work

Xu et al. [5] studied the Industrial IoT applications and their challenges also highlighted the possible research opportunities for the researchers in the future. Mendez et al. [6] presented a survey of the privacy and security methods and the changes related to Industrial IoT systems. Their work focused on the Industrial IoT technologies and architectures as well as on different security challenges (such as, availability, confidentiality and integrity) in different industrial communication layers. Husamuddin and Qayyum [7] studied the Industrial IoT different applications and the security threads. They gave different examples about IoT such as infrastructure management, environmental monitoring, infrastructure management, manufacturing, home automation, transportation, medical and health care systems. In order to understand and identify the critical scopes where IoT is used heavily, Rizvi et al. [8] explained the challenges and requirements related to IoT security and the current security solutions that are proposed and implemented. Also, the authors discussed some of the factors such as the cost of security implementation solutions, data size and vulnerabilities of data collected and transmitted.

Hassija et al. [9] presented different security trends and their threats on different layers of IoT applications. The layers covered in such study were application layer, gateways, middleware layer, network layer and sensing layer. The authors discussed also the possible solutions for securing the IoT systems such as fog computing, blockchain, machine learning and edge computing. El bekkali et al. [10] surveyed a common architecture and most basic proposals for IoT systems and their security analysis related to each IoT layer. The authors presented solutions for IoT security issues at each IoT layer and made a comparison between those solutions to clarify the limitations of each security method. At the end of their paper, they gave some trends for future work. The success of any Industrial IoT system is based on the robustness of the cyber-physical manufacturing systems because of the huge amount of real-time data that needs to be exchanged during manufacturing processes. To achieve a good real-time processing and data transmission, the system needs to transmit data with high data rate, low latency, high coverage and high reliability. To achieve these characteristics, Cheng et al. [11] proposed an Industrial IoT system based on 5G wireless communication technology. In addition, they implemented different manufacturing technologies and manufacturing scenarios under different circumstances. Kumar and Iyer [12] analyzed how Industrial IoT can be used to increase profit in industrial processes and improve customer value. In their paper, they collected data from different journals and web sources. Then, they identified different challenges when implementing an Industrial IoT system.

Furthermore, the authors presented different communication protocols that can be used with the Industrial IoT to insure high level of security, such as, Open Platform Communication (OPC), Message Queue Telemetry Transport (MQTT), MODBUS, Constrained Application Protocol (CoAP), Process Field Bus (PROFIBUS) and International Society of Automation (ISA). Raposo et al. [13] proposed a study on a wireless sensor network (WSN) monitoring architecture to identify the limitation of industrial process automation technologies. In addition, the study included some deep insight into metrics, management protocols, techniques and different standards usable to industrial WSNs. Their study shows that the proposed architecture can possess the following properties: no increase in the cost of the node manufacturing, negligible effect in the main sensor node application, negligible effect on the bandwidth, negligible effect on the hardware components and finally no significant increase in energy consumption. Table 1 shows a comparison between different surveyed papers according to the security issue threat types, security solutions, Industrial IoT applications and IoT Communication Protocols.

Table 1. Comparison between different papers according to their contents.

Authors and Paper References	Paper Contents				
	Security Threats	Security Solutions	Levels of Threat and Security	Industrial IoT Applications	IoT Communication Protocols
Xu *et al.* [5]	NO	NO	NO	YES	NO
Mendez *et al.* [6]	YES	YES	YES	NO	YES
M. Husamuddin *et al.* [7]	YES	YES	NO	YES	NO

Rizvi *et al.* [8]	YES	NO	YES	NO	NO
Hassija *et al.* [9]	YES	YES	YES	YES	YES
El bekkali *et al.* [10]	YES	YES	YES	NO	NO
Cheng *et al.* [11]	NO	NO	NO	YES	YES
Kumar *et al.* [12]	NO	NO	NO	YES	YES
Raposo *et al.* [13]	NO	NO	NO	NO	YES

3. POSSIBLE ATTACKS ON INDUSTRIAL IOT AND THEIR COUNTERMEASURES

This section discusses the possible attacks on Industrial IoT and their countermeasures. These attacks can be found in one of five forms: Distributed Denial of Service, Eavesdropping, Man-in-the-Middle, Virus, Trojan Horse and Worm Virus.

3.1. Distributed denial of service (DDoS) attack

It is a common type of attack which decreases the service availability for both service provider and users. The DDoS attacker tries to flood the network with malicious packets in order to exhaust the network and their power suppliers. The DDoS attacker can attack both wired and wireless networks and as a result, the legitimate users cannot access services provided from the servers [14], [15].

3.2. Eavesdropping attack

This type of attack is possible when there is no secure channel between two end points or when using a weak security protocol. In this type, the attacker attacks the confidentiality of the data transferred, for example, between a client and a server. This attack is not easy to detect because the attacker sniffs the transferred packets on the LANs or intercept the wireless communication channels without alternating data and the system continues working as usual. This type of attack can be established by using network monitoring software in order to intercept the transferred data. Besides network analysis, Eavesdropping can listen to the Industrial IoT devices, mobile devices, servers and clients. To reduce the possibility of eavesdropping attack, many actions and means can work such as using an encryption between two end points, updating the applications and devices, or by using software protections (anti-virus, Firewalls, antimalware, VPNs, etc.) [16]-[17].

3.3. Man-in-the-middle (MITM) attack

It is a type of cyberattack in which an unauthorized person gets in the link between two parties and controls a session between them by changing the contents of messages or producing extremely new messages. The attacker tries to trick both communicating parties and give an illusion to both of them that they are communicating to each other. Therefore, MITM attacks the confidentiality and integrity of the sessions. This type of attack can be achieved by two steps, interception and decryption. To protect against MITM attacks, a number of proactive steps should be taken before discovering that MITM attacks become too late [18], [19]. The best ways to prevent MITM are: active searching to detect if the communication link has been intercepted, using strong WEP/WPA encryption on Access Points, Strong Router Login Credentials, Virtual Private Network, HTTPS and Public Key Pair Based Authentication [20], [21].

3.4. Virus attack

A virus is a malicious code that is injected by the attacker to be executed on the host computer. The viruses have the ability to self-install and self-replicate within a short period of time. The virus manipulates the access control mechanism of the host device to decrease the system performance, decrease availability, and make the system consume unreasonable amounts of processing power or network bandwidth [22], [23]. To immune the system against viruses, several steps should be taken into consideration such as: using strong passwords, keeping the system up to date, applying antivirus software, using firewall, installing popup blocker, knowing the signs of infection and awareness of email phishing scams.

3.5. Trojan horse virus

A Trojan is a type of virus that looks like a normal computer program but a malicious functionality is hidden inside. The Trojan cannot start working without initial permission from the computer user because it is an executable file. A Trojan designed to attack the host computer after some time by disabling applications, destroying the system, allowing illegitimate remote access, illegitimate data send or security software disable [24], [25]. To protect the system from this type of attack, the user should follow the following steps [26]:

- Installing cyber-security software.
- Using trusted suppliers to download or install software.

- Never installing or opening an attachment file that is sent by an unknown sender.
- Updating all the computer software's and operating system.
- Installing and running a Trajan antivirus.

3.6. Worm virus attack

The worm is a malicious virus that has the ability to replicate itself and spread-out through the network in an automatic way. This virus exploits the weaknesses in the host system to corrupt files, leak sensitive information or open a small hole in a system to allow illegitimate access to that system. The worms exhaust the system memory and the network bandwidth by overloading them. This virus is more harmful than the traditional viruses because firstly, it can start the attack on its own without needing a host computer like the traditional viruses. Secondly, the attack can start without human intervention [27]. In order to protect against worm virus, the operating system should be updated, never openinng untrusted links from the internet, using anti-virus and anti-malware [28].

4. SECURITY AND PRIVACY CHALLENGES IN INDUSTRIAL IOT

Recently, there is an enormous increase in data exchange through the internet which, notably, increases the number of cyber physical systems which are mainly dependent on a strong connectivity and availability of the internet. The cyber physical systems include industrial systems, smart vehicles, and smart buildings. In general, different standard systems need to be interacting with each other in real-time by exchanging a huge amount of critical- sensitive data. The systems should guarantee the privacy, security and standardization of data which is an attractive target to attackers. In Industrial IoT systems, beside the previous security issues, the most important factor is availability because the whole production line will stop if the connection between any two parts of the system is blocked or delayed [29].

4.1. Security trends for cyber physical production systems (CPPS) and classical information technology (IT) system

The security of Industrial IoT applications are unlike the typical IT systems because these applications affect physical equipment and devices which may be dangerous to human life and safety. Also, Industrial IoT systems contain many different devices that can operate with their own operating system and applications which are different from the typical IT systems. Another issue is that the Industrial IoT is a real-time operating system (RTOS) which exposes to memory allocation as a critical problem unlike the typical IT Systems. At the field level, there are many embedded systems that run for a long time, maybe for years, with accumulating fragmentation and without rebooting. For this reason, the problem of buffer overflow may arise compared to typical IT systems [30].

In the industrial field, the technology that deals with the industrial data is called Operational Technology (OT). OT refers to the relation between hardware and software which are designed to control a specific hardware system, for instance, monitor mechanical performance, control heat, sewage systems, water distribution, etc., whereas IT is related to the network applications, data exchange between organizations, data storage, etc. In Industrial IoT environments, OT and IT are both used together where the OT's are used to control the physical devices and the IT's are used to deal with the information. The integration of OT and IT supports industries with better performance to optimize the automation. This convergence makes the Industrial IoT systems more susceptible to cyberattacks [31]-[33]. Fig. 2 shows the convergence between OT and IT.

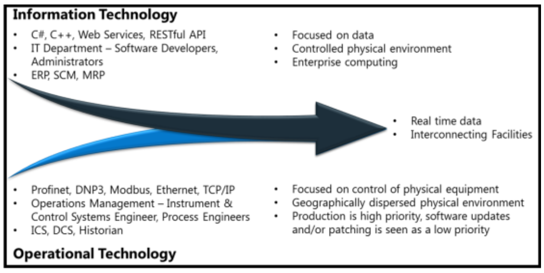
Information Technology
• C#, C++, Web Services, RESTful API
• IT Department – Software Developers, Administrators
• ERP, SCM, MRP
• Focused on data
• Controlled physical environment
• Enterprise computing
• Real time data
• Interconnecting Facilities
• Profinet, DNP3, Modbus, Ethernet, TCP/IP
• Operations Management – Instrument & Control Systems Engineer, Process Engineers
• ICS, DCS, Historian
• Focused on control of physical equipment
• Geographically dispersed physical environment
• Production is high priority, software updates and/or patching is seen as a low priority
Operational Technology

Fig. 2. Convergence of IT and OT [31].

The bad effects of cyber-attack on CPPS can appear in the following forms [2], [31]:

- Information delay from a client to the server or vice versa.
- Connection interruption between client and server to start an action through a safety system.
- Altering the received value coming from the client side, which may lead to automatic response, for instance, automatically shutting down a section of a factory or giving an instruction to a worker to do inappropriate action.
- Altering the set point of application at the client side, for instance, changing the alarm

level sensor point for an oil tank to exceed the maximum level.

- Modifying/changing the maximum or minimum operation protection values for a system, for example, increasing the maximum rotation speed limit of a turbine in a plant to destroy the blades of it.

4.2. Operational technology and information technology possible attacks

Any Industrial IoT system can be divided into five layers, each layer may expose to different types of cyber-attacks. Table 2 shows those five layers and their possible attacks. The five layers are grouped into two parts: the first three layers are form the operational technology (OT), whereas the upper two layers are form the information technology (IT).

The first level of the Industrial IoT includes the physical parts of systems such as, sensors, actuators, motors, transmitters and embedded devices. The attacker usually needs a full knowledge about this level to be able to start his/her attacks. For example, the attacker should know the active devices specifications, devices operational functionality, devices installation functionality and engineering planets.

The second level of Industrial IoT includes the control devices which are responsible for collecting data from the first level and taking an appropriate action according to the information coming from the upper layers. The control devices are: gateways, programmable logic control (PLCs) and distributed control systems (DCS). At this layer, the attacker tries to prevent the communication with the lower level or control the flow of data.

The third level of Industrial IoT is the Supervisory Control and Data Acquisition (SCADA). This layer consists of the following components: master stations, human interface machines (HMIs), data acquisition devices, network connectivity and databases. Usually all the devices at this layer communicate via the Ethernet cables using the IP protocol. At his layer, the attackers depend on IP creation methods. For example, an IP with the sender address can be created to give an illusion to the receiver that the source of this packet comes from a legitimate user.

The fourth level of Industrial IoT contains business planning services. For instance, web services, mail services, intranet, office applications. The attacker at this layer exploits vulnerabilities in the services to inject a malicious code that generates fake data to give an illusion to the application that these data come from a legitimate user to get access with administrator privilege.

The fifth level of Industrial IoT is the higher layer of the industrial pyramid which includes enterprise applications to handle data mining, cloud computing, and analytics services. The attacker at this layer aims to intercept data, trick the system, noting that there are more advanced types of attacks like adversarial attacks [33], [34].

Table2. Layered Industrial IoT architecture and possible attacks [35].

Layer		Components	Possible Attacks
IT	V	Business Applications, Internet, Cloud Computing, Data Analytics, and mobile Devices.	DoS, side channel attacks, Cloud malware Injection, Authentication attacks, Man-in-the-Middle, and Mobile device attacks.
	IV	Data Centres, Intranet, Mail, Office Applications, and Web Services.	Phishing, Malware, DNS, SQL Injections, poisoning, Brute Force attack, Remote code Execution, and Web Application attacks.
DeMilitarized Zoon			
OT	III	SCADA Control, HMI, Control Room, and Operator Stations	IP spoofing, Data manipulation, Data sniffing, Malwares.
	II	Distributed Control System, PLC, and Gateways.	Replay attack, Sniffing, Man-in-the-Middle attack, Brute force Password guessing, and Wireless device attack.
	I	Sensor, Motors, Actuators, Transmitters, Embedded Devices.	Reverse Engineering, injecting crafted packages or input, Malware, Eavesdropping, and Brute-force search attacks.

It should be noted that Table 2 shows a demilitarized zone located between the third and the fourth layers which represents untrusted network servers that the users are connected to when using an untrusted network.

4.3. Security challenges for Industrial IoT

Besides the ordinary security issues mentioned in section 3 above, there are other security challenges that should be considered when designing an industrial IoT system. The additional challenges are platform security, security management, secure engineering, identity management and industrial rights management. The solution for the mentioned challenges must continue for the whole life cycle of the designed system. The additional security properties that must be taken into account are [36]:

- Industrial IoT devices need to be tamper resistant to prevent potential physical attacks, such as passive secret stealing and unauthorized re-programming while allowing the update of security firmware on devices by authorized users.

- The Industrial IoT device storage data should be encrypted to keep the data protected from adversaries and to achieve confidentiality.
- The Industrial IoT communication network should be secured to keep integrity and confidentiality.
- The infrastructure of the Industrial IoT needs efficient authorization and identification mechanisms to guarantee that only authorized entities can access the industrial IoT resources.
- Redundancy in hardware devices and communication links must be used to ensure the availability of the Industrial IoT system with normal operation even when a physical damage happens by malicious users.

5. APPROACHES TO SECURING THE INDUSTRIAL IOT

In Industrial IoT systems, securing the data is very important because it is related to human safety and life. But using ordinary secure methods such as, authentication control systems and encryption algorithms are insufficient since hackers' become more skilled with hand powerful processors to access and manipulate data. For this reason, another securing method should be added through the different Industrial IoT architecture levels. The security can be increased by using Communication Management, Access Control, Data Encryption, Data Auditing and Monitoring [37], [38].

5.1. Communication management

The control and the monitor of data flow between different layers is very important to ensure the security of data especially when the data is very important. The security provided by the data management prevents adversaries from attacking confidentiality and integrity of the data. It also prevents manipulation and data leakage attacks such as man in the middle, eavesdropping and other possible attacks on the communication mediums. As a precaution, communication management can create policies to secure information, detect and identify security threats on the industrial system [39], [40].

5.2. Access control

It is the mechanism to guarantee the identity of a subject or a user that is willing to access a remote resource. There are different items that can be used to describe Access Control like Authorization and Privilege Handling.

Authorization is known as the process of allowing access of a specific subject to a specific object. To design an effective access control system, a secure entity identification is required. Privilege escalation attack or elevation of privilege is an attack that exploits a bug in the application software, or operating system to access protected resources. The effect of this action is that unauthorized attackers can access and modify an application with more privileges than system administrator, or application developer can do [41], [42].

5.3. Data encryption

It is used to convert readable information into unreadable form by using one of the encryption techniques. There are two main types of encryptions: symmetric encryption and asymmetric encryption. In symmetric encryption, the same encryption key is used for encryption and decryption. Whereas in asymmetric keys, two different keys are used; one for encryption and other for decryption. When using encryption techniques, even though the attacker passes the access method, it is still unable to read the data unless the attacker has the decryption key [43]-[45].

5.4. Data auditing and monitoring

It is the operation of verifying data by using a specific regulation and rules to protect against data leakage, malware, data tampers and misconfiguration. In order to prevent data leakage, a hardware based cryptographic tamper proof with tamper resistance is used. For Industrial IoT applications, other resistance tampering methods are used to insure the security of the information such as misconfiguration and reverse engineering. The data auditing has the following benefits [46]-[48]:

- The capability to detect risks related to data irretrievability and loss.
- Providing a method to evaluate and observe operations of the audited client.
- Reducing the percentage of security violations.
- Detecting gaps in the cyber security system and their drawbacks.

6. CONCLUSIOINS

Industrial IoT has grown significantly in recent years because of the huge increase in internet services. The Industrial IoT applications are mainly dependent on the data communication between nodes through the internet. The industrial data is real-time data which needs a high data rate with a good quality of service to be transferred.

The data transferred from the sensor layer to the upper layers may hold sensitive data which need to be protected from unauthorized access. Therefore, the security of the Industrial IoT systems is a critical factor in industry because successful attacks on the system can cost the companies or governments a huge loss. The attackers may steal data, deny the service or cause physical damage.To guarantee the security of the communication between any two nodes, Industrial IoT should have protection services such as encryption, authentication, access control, data auditing and monitoring. In this paper, Industrial IoT possible cyber security attacks have been investigated in addition to their different Industrial IoT communication layers and the possible method to protect against cyber-attacks.Challenges regarding security of Industrial IoT systems and their solutions in addition to the challenges of the conventional IT systems are: platform security, security management, secure engineering, identity management and industrial rights management. As a result, the Industrial IoT system requires higher level of security protection.

REFERENCES

[1] D. Dzung, M. Naedele, T. P. Von Hoff, and M. Crevatin, “Security for industrial communication systems,” *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1152–1177, 2005.

[2] Z. Bakhshi, A. Balador and J. Mustafa, "Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models," in *IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, 2018, pp. 173-178.

[3] S. Vitturi, C. Zunino and T. Sauter, "Industrial Communication Systems and Their Future Challenges: Next-Generation Ethernet, IIoT, and 5G," *Proceedings of the IEEE*, vol. 107, no. 6, pp. 944-961, 2019,

[4] P. Jie and L. Li, "Industrial Control System Security," in *Third International Conference on Intelligent Human-Machine Systems and Cybernetics*, 2011, pp. 156-158.

[5] L. D. Xu, W. He and S. Li, "Internet of Things in Industries: A Survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no 4, pp. 2233-2243, 2014.

[6] D. Mendez, I, Papapanagiotou, and B. Yang,"Internet of things: Survey on security and privacy," *Information Security Journal: A Global Perspective*, pp. 1-16, 2017.

[7] M. Husamuddin and M. Qayyum, "Internet of Things: A study on security and privacy threats," in *2nd International Conference on Anti-Cyber Crimes (ICACC)*, 2017, pp. 93-97.

[8] S. Rizvi, A. Kurtz, J. Pfeffer and M. Rizvi, "Securing the Internet of Things (IoT): A Security Taxonomy for IoT," in *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018, pp. 163-168.

[9] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, pp. 82721-82743, 2019.

[10] A. El bekkali, M. Boulmalf, M. Essaaidi, and G. Mezzour,"Securing the Internet of Things (IoT): Systematic Literature Review," *Computing Community Consortium (CCC)*, pp. 1–6, 2019.

[11] J. Cheng, W. Chen, F. Tao, and C. Lin,"Industrial IoT in 5G environment towards smart manufacturing," *Journal of Industrial Information Integration*, vol. 10, pp. 10-19, 2018.

[12] A. S. Kumar and E. Iyer, “An industrial iot in engineering and manufacturing industries—benefits and challenges,” *International journal of mechanical and production engineering research and dvelopment (IJMPERD)*, vol. 9, no. 2, pp. 151–160, 2019.

[13] D. Raposo, A. Rodrigues, S. Sinche, J. Sá Silva, and F. Boavida, "Industrial IoT Monitoring: Technologies and Architecture Proposal,". *Sensors*, vol. 18, no. 10, 2018.

[14] K. N. Mallikarjunan, K. Muthupriya and S. M. Shalinie, "A survey of distributed denial of service attack," in *10th International Conference on Intelligent Systems and Control (ISCO)*, 2016, pp. 1-6.

[15] A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586-602, 2017.

[16] H. -N. Dai, H. Wang, H. Xiao, X. Li and Q. Wang, "On Eavesdropping Attacks in Wireless Networks," in *IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES)*, 2016, pp. 138-141.

[17] D. Xu, H. Zhu and Q. Li, "Jammer-Assisted Legitimate Eavesdropping in Wireless Powered Suspicious Communication Networks," *IEEE Access*, vol. 7, pp. 20363-20380, 2019.

[18] A. Mallik, A. Ahsan, M. Shahadat, and J. Tsou, "Man-in-the-middle-attack: Understanding in simple words, " *International Journal of Data and Network Science*, vol. 3, no. 2, pp. 77–92, 2019.

[19] A. R. Chordiya, S. Majumder and A. Y. Javaid, "Man-in-the-Middle (MITM) Attack Based Hijacking of HTTP Traffic Using Open Source Tools," in *IEEE International Conference on*

Electro/Information Technology (EIT), 2018, pp. 0438-0443.

[20] I. Butun, P. Österberg and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616-644, 2020.

[21] Rapid7. (2017). Man in the Middle (MITM) Attacks | Types, Techniques, and Prevention, [Online] Available: https://www.rapid7.com.

[22] A. Ilmudeen, "The impact of computer virus attacks and its preventive mechanisms among personal computer (PC) users," *Semantic Scholar*, pp. 97-103, 2013.

[23] H. A. Khan, A. Syed, A. Mohammad and M. N. Halgamuge, "Computer virus and protection methods using lab analysis," in *IEEE 2nd International Conference on Big Data Analysis (ICBDA)*, 2017, pp. 882-886.

[24] V. K. Gudipati, A. Vetwal, V. Kumar, A. Adeniyi, and A. Abuzneid, “Detection of Trojan Horses by the analysis of system behavior and data packets,” in *Long Island Systems, Applications and Technology*, 2015, pp. 1–4.

[25] M. Tehranipoor and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 10-25, 2010.

[26] Webroot. (2022). What is a Trojan Virus. [Online]. Available: https://www.webroot.com.

[27] L. Xue and Z. Hu, "Research of Worm Intrusion Detection Algorithm Based on Statistical Classification Technology," in *8th International Symposium on Computational Intelligence and Design (ISCID)*, 2015, pp. 413-416.

[28] N. Weaver, V. Paxson, S. Staniford, and R. Cunningham, “A taxonomy of computer worms,” in *Proceedings of the 2003 ACM workshop on Rapid Malcode*, 2003, pp. 11–18.

[29] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, “Security and privacy challenges in industrial internet of things,” in *Proceedings of the 52nd annual design automation conference*, 2015, pp. 1–6.

[30] B. Zhu, A. Joseph and S. Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," in *International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, 2011, pp. 380-388.

[31] G. Murray, M. N. Johnstone, and C. Valli, "THE CONVERGENCE OF IT AND OT IN CRITICAL INFRASTRUCTURE," in *Australian Information Security Management Conference*, 2017, pp. 149-155.

[32] Coolfiresolutions. (2019). What Is The Difference Between IT and OT.[Online] Available: https://www.coolfiresolutions.com

[33] Cymune. (2019). Industrial IoT (Industrial IoT) and Operational Technology (OT) Security challenges [Online], Available: https://www.cymune.com.

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

[35] K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, "Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures," *IoT 2021*, vol. 2, no. 1, pp. 163-186, 2021.

[36] E. Sisinni, A. Saifullah, S. Han,U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724-4734, Nov. 2018.

[37] B. Sumitra, C. R. Pethuru, and M. Misbahuddin, "A Survey of Cloud Authentication Attacks and Solution Approaches," *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 2, no. 10, pp. 6245-6253, 2014

[38] J. Kuusijärvi, R. Savola, P. Savolainen, and A. Evesti, "Mitigating IoT security threats with a trusted Network element," in *International Conference for Internet Technology and Secured Transactions (ICITST)*, 2016, pp. 260-265.

[39] M. Furdek *et al.*, “An overview of security challenges in communication networks,” in *2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM)*, 2016, pp. 43–50.

[40] Blog.Netwrix. (2020). Data Security Management: Where to Start [Online], Available: https://blog.netwrix.com.

[41] B. Leander, *Access Control Models to secure Industry 4.0 Industrial Automation and Control Systems*. 2022.

[42] Q. Bai and Y. Zheng, "Study on the access control model," in *Proceedings of 2011 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference*, 2011, pp. 830-834.

[43] E. Khalaf, and M. M. Kadi, "A Survey of Access Control and Data Encryption for Database Security," *Journal of King Abdulaziz University-Engineering Sciences*, vol. 28, no. 1, pp. 19 – 30, Jan. 2017.

[44] I. Basharat, F. Azam, and A. W. Muzaffar, "Database Security and Encryption: A Survey Study," *International Journal of Computer Applications*, vol. 47, no. 12, pp. 28-34, 2012.

[45] Y. Kumar, R. Munjal, and H. Sharma, "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures,". *International Journal of Computer Science and Management Studies*, vol. 11, no. 3, pp. 60-63, Oct. 2011.

[46] J. Singh, T. Pasquier, J. Bacon, H. Ko and D. Eyers, "Twenty Security Considerations for Cloud-Supported Internet of Things," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 269-284, June 2016,

[47] S. Jones, S. Ross, and R. Ruusalepp, *Data Audit Framework Methodology*, version 1.8, Glasgow, HATII., 2009.

[48] T. Li and C. Liu, "Data “Audit” Research Based on the Accounting Information System," in *International Conference on E-Business and E-Government*, 2010, pp. 2416-2419.

تأمين إنترنت الأشياء الصناعية- مراجعة للتحديات والحلول

محمد باسل شكر*
mohammed.enp95@student.uomosul.edu.iq

جاسم محمد عبد الجبار**
drjssm@almaaqal.edu.iq

*جامعة الموصل - كلية الهندسة - قسم هندسة الحاسوب - موصل - العراق
**جامعة المعقل – كلية الهندسة – قسم هندسة السيطرة والحاسبات- البصرة - العراق

تاريخ الاستلام:19-08-2022 استلم بصيغته المنقحة: 27-09-2022 تاريخ القبول22-10-2022

الملخص

إنترنت الأشياء الصناعي هي تقنية جديدة واعدة يمكن استخدامها لزيادة كمية وجودة المنتجات الصناعية. تضمن تقنيات إنترنت الأشياء الصناعية التحكم الكامل في العمليات الصناعية والانتاجية عن بُعد من خلال الإنترنت والتي يمكن أن تقلل من عدد العاملين في المصانع والمعامل مما يقلل من نسبة الإصابات والحوادث اثناء العمل بالإضافة إلى تقليل التكاليف الإجمالية. تعد أنظمة إنترنت الأشياء الصناعية من الأهداف الجذابة لقراصنة المعلومات ولهذا السبب تتطلب هذه الأنظمة مستويات عالية من الأمان لأن هذه الانظمة لها تأثيرات مباشرة على الأجهزة المادية التي قد تكون مصدر خطورة على حياة الإنسان وسلامته في حال تعرضها لهجوم إلكتروني خارجي. ولضمان مستوى عالٍ من الأمان، يجب أن يتم الجمع بين تكنولوجيا المعلومات(IT) *والتكنولوجيا التشغيلية* (OT) *والأساليب المبتكرة الجديدة. في هذا البحث مراجعة للعديد من التقنيات الجديدة وطرق الأمان مع الهجمات المحتملة عليها من أجل تزويد مصممي البنية التحتية لإنترنت الأشياء الصناعية بالمعلومات المطلوبة لأخذها بنظر الاعتبار. أيضًا، تم التحقق من الاختلافات والمقاربات بين كل من تكنولوجيا المعلومات الكلاسيكية والتكنولوجيا التشغيلية وعلاقتهما بأنظمة إنترنت الأشياء الصناعية مع الهجمات المحتملة على كل طبقة من طبقات تكنولوجيا المعلومات والتكنولوجيا التشغيلية.*

الكلمات الداله:

الهيكل الموحد (OPC UA) ،إنترنت الأشياء الصناعية، تكنولوجيا المعلومات، التكنولوجيا التشغيلية، نظام التحكم الإشرافي وتحصيل البيانات (SCADA)، القرصنة الالكترونية.