# Researching Cyberattacks Methods in Industrial Internet of Things

Vladyslav Yevsieiev[1], Nataliia Demska[1]

1. CITAM Department, Kharkiv National University of Radio Electronics, UKRAINE,
Kharkiv, Nauky Ave. 14., e-mail: vladyslav.yevsieiv@nure.ua

***Abstract*:** This work is devoted to the study of modern methods of protecting the access to corporate information in modern Smart Manufacturing built on the basis of IIoT. The authors conduct a comparative analysis of vulnerabilities in IIoT networks, consider the security issues of cyber-physical production systems in Industry 4.0.

***Keywords*:** Industry 4.0, Smart Manufacturing, Industrial Internet of Things, cyberattacks, cybersecurity.

## I. Introduction

Modern high-tech production is not possible without the use of Industry 4.0 concepts, which is based on the use of the Industrial Internet of Things (IIoT) to create Smart Manufacturing [1]. Which allows the development of a cyber-physical production system (CPPS) that automates the production process using Machine-to-Machine (M2M) technologies [2]. In a highly competitive environment, CPPS in Industry 4.0 are susceptible to cyberattacks [3]. There are various vulnerabilities in CPPS, and they exist at the levels of information exchange. Supervisory Control And Data Acquisition (SCADA) systems refer to industrial computer systems that control the flow of the technological process, the quality and stability of production depends on the reliability of the data received and the decisions made. Analyzing security vulnerabilities in SCADA systems, the following can be distinguished [4]: network and communication protocols; Program logic controllers (PLC); database or application servers; Remote terminal (RT); Human-machine interfaces (HMI).

As you can see from the dedicated list of vulnerabilities for cyberattacks, it is necessary to implement various protection mechanisms for the smooth functioning of production processes. Safe data transmission is the main aspect of CPPS, the problem of insecurity arises due to the leakage of account data, passwords, hacking of local networks, through poor-quality access passwords to them, the human factor, the introduction of keyloggers on both remote terminals and stationary PCs. As a result of such attacks, which lead to intruders gaining access to production information, and with some success, they can gain access to corporate information that is stored in the cloud server of the enterprise. All these actions can lead to distortion of current production information, to the loss of new technologies, which leads to large financial losses. As a result, research and development of new software and hardware methods for protecting access SCADA / HMI in CPPS is one of the key forms of protection against Cyberattacks.

## II. Analysis of IoT architecture and vulnerabilities

IIoT is a real-time communication between sensors and a control system. In the IIoT architecture, which is built on the basis of the Internet of Things (IoT) architecture, it has 3 levels of architecture [5]. In work [6] these levels and risks and threats of cyberattacks on them are considered, the result is presented in table 1.

Table 1. Risks and threats of cyberattacks in IIoT

| **IIoT layer** | **Security Threats** |
|---|---|
| Physical (Sensor,PLS ) | Tampering, Denial of Service |
| Networking (M2M) | Passive Monitoring, Eavesdropping |
| Application (SCADA/HMI) | Integrity, Modification |

At this point in time, more than 20-24 percent of the total number of IIoT devices in production work on the Internet. The use of IIoT devices is growing rapidly. The problem is that this growth leads to the emergence of various vulnerabilities that make these devices less secure [7].

The protection of the privacy and security of production data due to certain risks and vulnerabilities posed by cyberattacks, is called cybersecurity. The priority of cybersecurity is to protect the integrity, availability and confidentiality of data [8]. The purpose of cyberattacks is to block services, get unauthorized access to data, information disclosure, copying, sale, use and destruction, which leads to large financial losses. In [9] the following grouping of cyberattacks is proposed: Vulnerability and Penetration Test; Sniffing; Phishing; E-mail spam; Malicious software: Virus, Adware, Trojan, Worm, Spywar. [10-12]. Based on this, enterprises that implement the concept of Industry 4.0 in the form of CPPS should take into account the standards for information security management ISO / IEC 27001 [13], as well as in which measures to prevent and protect against cyberattacks are defined. Analyzing the standards, the following can be distinguished, that when implementing the information security policy, it is necessary to take into account the following aspects: environmental and physical safety; communication security; access control; use of cryptographic controls; protection from malicious software. Considering aspects such as access control, use of cryptographic controls, you can see that when using IoT technologies, you can use several communication protocols in control systems in various areas of the enterprise. But in the conditions of the IoT, they are divided into open and closed. For example, communication between vendor independent

devices is observed in open systems communication protocols, while communication between manufacturer's own devices is observed in closed systems communication protocols. In real production conditions, remote monitoring, as well as control of large-scale systems, is provided by SCADA / HMI. SCADA / HMI safety standards, API 1164 [11] describes Profinet, DNP3 and Modbus protocols. Cyberattacks for these protocols, inside IIoT are hardly possible. But it should be noted that end users, operators, can use the IoT for remote monitoring and control of technological processes via SCADA / HMI, which is located in the cloud storage. As a result, the user does not use the protected corporate network of the enterprise, but the global Internet networks. One of the biggest threats is that the user and the attacker are on the same network. As a result, it is possible to steal access passwords to the enterprise cloud, as well as direct access to SCADA / HMI, remote terminals, which can lead to irreparable damage to the production process at enterprises. There are two main methods of stealing access passwords:

Phishing Attack - a method of fake sites, an attacker fakes the site of organizations or institutions. The user is sent a link in an e-mail in the form of setting tasks or the occurrence of a production need and is prompted to follow it to solve the problem. In this case, the user in a hurry enters the forged site of the enterprise and enters his username and password. As a consequence, the attacker gains access to the corporate network of the enterprise and the files that are available to this account.

Social Engineering - in this case, an attacker deceives the user according to a certain scenario. In social engineering, an attacker uses his abilities to convince a user to enter the required data. In the study of social engineering attacks, different methods are used [12]. We list only the main ones: fake goods and services; mobile phones; Trojan's viruses.

The above methods of stealing data from the Application layer of IIoT are not a complete list, but are presented as the main ones. In the work of Mamoona Humayuna, NZ Jhanjhi [13], the following Cyber-attacks targeting Application layer of (SCADA / HMI) methods are considered which are presented in Figure 1.

Based on this, it can be concluded that the Application layer is very vulnerable to Cyberattacks due to the human factor, the form of loss or disclosure of Logins and passwords to access corporate information, which leads to the following negative results:

- decreased productivity, collisions in decision making in production control devices, loss of data, interruptions in their provision in real time.

- Industry 4.0 uses IoT devices that are vulnerable to cyber attacks, which makes the entire system vulnerable, and this negatively affects the coordination and exchange of data between devices and operators, data synchronization is disrupted.

- CPPS is not secure from risk and can face various challenges due to cyber attacks. This can cause an abrupt halt in the operation of the entire system, an interruption in the transfer of data from sensors through the PLC to the SCADA / HMI, which can lead to a halt in production.

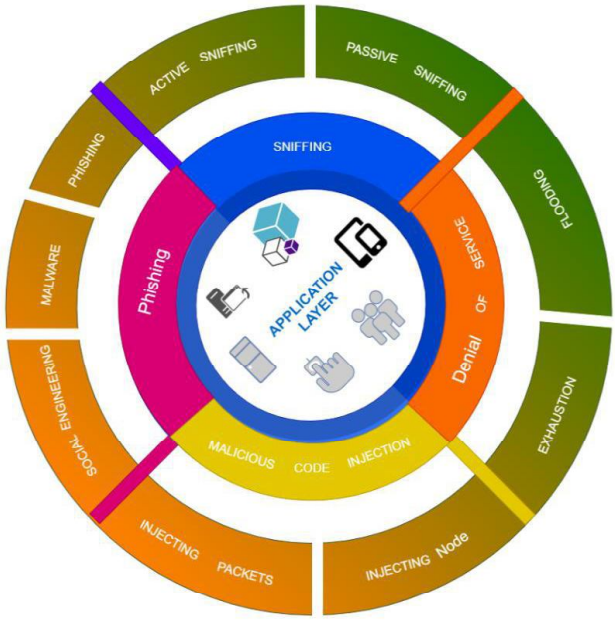


Fig.1. Cyber-attacks targeting Application layer of SCADA/HMI [14]

As a result, the authors propose a new strategy for protecting against theft of access passwords, which will allow Cyberattacks to be avoided using the following methods: Sniffing attack; Denial of Service (DDoS); Code Injection.

After analyzing the potential threats that can be carried out by the Application layer of (SCADA / HMI), it is necessary to develop new measures to protect users from data loss. To do this, the authors propose to implement the following main theses of protecting the user from disclosure and data loss for authorizations in IIoT via the Internet.

- restrict the user from knowing his password and login;

- complicate the password and not associate it with specific dates or associative concepts of the user, automatic generation of username and password;

- change of username and password less than once a week, automatically, without notifying the user;

- provide automatic login information without using a keyboard, thus avoiding the use of keyloggers and similar spyware;

- automatic check of the URL where the user enters, to ensure protection against Phishing Attack;

- implement two-factor user authentication.

Analyzing the proposed theses, it can concluded that this will be a complex software and hardware protection based on the use of modern microcontrollers, which will provide reliable data storage even when trying to hack information, create a "dump" of firmware or loss of a device.

## III. Conclusion

The study of methods of protecting access to information in IIoT networks showed a number of vulnerabilities to cyber attacks on the Application layer of SCADA / HMI. One of the critical vulnerabilities is a person who interacts with Smart Manufacturing through remote access to SCADA / HMI, enterprise cloud services, through standard identification

methods (login and password). The most common theft methods such as Phishing Attack, Social Engineering, and keyloggers were analyzed. The reasons for their operation are considered, which lie in the psychology and not attentiveness of the user, when entering data. To increase the level of data protection against such types of cyberattacks, the authors propose new theses for expanding protection, in the form of developing a hardware and software complex that automates site verification, entering a login and password, while eliminating the disclosure of data or determining them by associative prerequisites (dates of birth, names animals, nicknames, etc.) because the user himself will not know the passwords.

This research is a promising direction in the field of cybersecurity within the CPPS for Smart Manufacturing, as well as for other Industry 4.0 areas in which IIoT and IoT are used.

## REFERENCES


[1] Nevliudov, I., Yevsieiev, V., Demska, N. and Novoselov, S. (2020) "DEVELOPMENT OF A SOFTWARE MODULE FOR OPERATIONAL DISPATCH CONTROL OF PRODUCTION BASED ON CYBER-PHYSICAL CONTROL SYSTEMS", INNOVATIVE TECHNOLOGIES AND SCIENTIFIC SOLUTIONS FOR INDUSTRIES, (4 (14), pp. 155-168. doi: 10.30837/ITSSI.2020.14.155.

[2] Ramjee Prasad, Vandana Rohokale. (2019). Internet of Things (IoT) and Machine to Machine (M2M) Communication. Cyber Security: The Lifeline of Information and Communication Technology pp 125-141. DOI: 10.1007/978-3-030-31703-4_9.

[3] K. Zhou, T. Liu, and L. Zhou. (2015). Industry 4.0: Towards future industrial opportunities and challenges, In Fuzzy Systems and Knowledge Discovery (FSKD), 12th International Conference, p.2147-2152.

[4] M. Lezzi, M. Lazoi, and A. Corallo. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework, Computers in Industry, 103, 97-110

[5] P. Varga, S. Plosz, G. Soos, C. Hegedus. (2017). Security Threats and Issues in Automation IoT, IEEE International Workshop on Factory Communication Systems conference, Trondheim, Norway, 6.

[6] D. Pancaroğlu. (2018). An Analysis of the Current State of Security in the Internet of Things, International Conference on Cyber Security and Computer Science (ICONCS'18), Safranbolu, Turkey.

[7] R. Von Solms, N. J. Van. (2013). From information security to cybersecurity, computers & security, 38, 97-102.

[8] M. Akin, S. Sağiroğlu, Gelişmiş Sürekli Tehditler, Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi , 10 (1) , 1-10, 2017.

[9] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits. (2012). Systematic analysis of cyber-attacks on CPS-evaluating applicability of DFD- based approach, In Resilient Control Systems (ISRCS), 5th International Symposium, 55-62, 2012.

[10] C. K. Chen, Z. K. Zhang, S. H. Lee, and S. Shieh, Penetration Testing in the IoT Age, Computer, 51(4), 82-85, 2018.

[11] H. Çakır, H. Yaşar, Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri, Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 3 (2), 488-507, 2015.

[12] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid. (2018). Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions, Computers & Security, 74, p. 144-166.

[13] ISO/IEC 27001 Information security management. [Electronic version]. https://www.iso.org/isoiec-27001-information-security.html. (Access date: 18.09.2021)

[11] API Standard 1164, 3rd Edition. Pipeline Control Systems Cybersecurity. [Electronic version]. https://www.api.org/products-and-services/standards/ important-standards-announcements/1164. (Access date: 18.09.2021).

[12] Berger, S., O. Bürger, and M. Röglinger. (2020). ATTACKS ON THE INDUSTRIAL INTERNET OF THINGS–DEVELOPMENT OF A MULTI-LAYER TAXONOMY. Computers & Security, p. 101790.

[13] Humayun, Mamoona, N. Z. Jhanjhi, Bushra Hamid, and Ghufran Ahmed. (2020). Emerging smart logistics and transportation using IoT and blockchain." IEEE Internet of Things Magazine 3, no. 2. P: 58-62.

[14] Mamoona Humayun, NZ Jhanjhi,Muhammad Nabil Talib, M H Shahd, G. Sussendran. (2021). Industry 4.0 and Cyber Security Issues and Challenges. Turkish Journal of Computer and Mathematics Education Vol.12 No.10. p. 2957-2971