*International Journal of Modern Agriculture, Volume 10, No.2, 2021*
*ISSN: 2305-7246*

# CYBERSECURITY – VULNERABILITY ASSESSMENT OF ATTACKS, CHALLENGES AND DEFENCE STRATEGIES IN INDUSTRY 4.0 ECOSYSTEM

**Saurabh Sharma[1], Tripti Dhote[2]**

[1,2] Symbiosis Institute of Digital and Telecom Management, Symbiosis International (Deemed University), Pune, India.
Email: [2]tdhote@sidtm.edu.in

**Abstract**

Technology along with its uses has increased the interconnected digital ecosystem. It also has heavy usage of data. When the data is in digital form, it is threatened by various cyber-attacks, which increases the need for cyber-security. Industry 4.0 has data as its basic fuel, therefore the vulnerability towards cyber-attacks increases in industry 4.0. In this study, we have identified various risks in the ecosystem of industry 4.0. Most evident vulnerabilities for cyber-security have been determined in control systems protocols, unable to manage network devices effectively, neglect of periodic infiltration tests, unprotected connections, and untrained personnel. In this study, these vulnerabilities are identified and cyber defense strategies are determined. The corporate and end-users are guided to implement preventions at the same time. The various vulnerabilities identified and their prevention will ensure that the damage from these vulnerabilities is minimal..

**Key words:** 4.0, Cyber Security, Vulnerability Assessment, Cyber Attack, Defence Strategies.

## Introduction

Many centuries ago, the invention of steam engines emerged as industry 1.0 [1]. The development of devices that are electrically powered emerged as Industry 2.0 [2]. The use of computers and robots for production emerged as industry 3.0 [3]. Intelligent manufacturing with minimal human influence along with the Internet of things, Artificial Intelligence, and Big data came to be known as industry 4.0. The Cyber-Physical Systems (CPS)are the structures that provide physical processes, computation, and networking by communicating with the physical world and the IIoT (Industrial Internet of Things) [3]. Intelligent systems used in manufacturing provide convenience but also lead to the risk of cyber-attacks [4]. The connections are either wireless or wired in Industry 4.0 networks. These networks are vulnerable to cyber-attacks and can have serious damages. Manufacturers who adopt Industry 4.0 must take care of various cyber risks and implement cyber-security strategies to avoid these risks [5]. The implementation during the installation phase is more helpful in defending cyber-attack risks than by applying defense strategies to an existing system [6]

## The Objective of the research

The objective of this study is to examine various cyber-security threats along with their defense strategies in the corporate as well as end-user aspects of industry 4.0 ecosystem. This study will help in preventing data losses and system failures. The first part describes primary data sources in Industry 4.0 that are the Cyber-physical systems and the IoT devices. These sources are further examined for potential cyber-attacks. Then, cyber-security preventions for these attacks are proposed. In the second part, the organizations have been advised to take defense strategies using information security policies and conduct cyber-security staff training. In the last part, the end-users have been informed about various cyber risks that can be avoided so that data and sensitive information theft can be prevented.

## Literature Review

In this study, the need for cyber-security is determined in the networks of industry 4.0. The Cyber-Physical Systems (CPS) is mainly affected in the Industry 4.0 by cyber-attacks [7] followed by IoT, manufacturing [8], and network layers [9]. Solutions are developed for these layers to minimize attacks [10].

There are various vulnerabilities in CPS and they are examined in the information exchange layers. TheSCADA

(Supervisory Control and Data Acquisition) systems refer to industrial computer systems that monitor and control a process. The areas of security vulnerabilities in the SCADA systems are as follows [10]:

- Network or communication protocols
- Program logic controllers
- Database or application servers
- Remote terminal units
- Human-machine interfaces

In communication between devices, the transfer of data securely is an important issue. When this data is hampered, various problems are generated regarding the functioning and processing of data. Therefore, the safety of IoT from various cyber-attacks devices needs to be considered. Due to these attacks, the organizations suffer reduced production which in turn decreases their competition in the industry. The organizations must address every possible risk and vulnerability due to these cyber-attacks to avoid the losses. It is also recommended to implement various defense mechanisms for the smooth functioning of the processes.Secure data transfer is the primary aspect of devices used for communication. The problem of insecurity is caused due to interruption to this data, modification, and deletion [11]. Unique and strong passwords should be created for the accounts. It is always advised to use a VPN to access wireless networks [12]. The end-users suffer data theft and financial losses in these attacks. In this study, various solutions to prevent cyber-attacks are proposed. These preventions are mainly aimed at specific layers or a single layer. The solutions for industry 4.0 are covered in this study.

**Research Methodology**

Firstly, we studied the Cyber-Physical Systems of industrial cyberspace and the IoT layers. We found out that these two are the primary data sources of Industry 4.0. Secondly, we learned about the various cyber-attacks that are present to infect these systems. We learned various concepts regarding the safety strategies of these systems. Thirdly, we learned about the importance of IoT devices and how these devices are essential to carry out industrial and manufacturing processes in industry 4.0. Then we examined various threats in the IoT layers and categorized them. Fourthly, we learned about cyber-security and its concepts. We studied various cyber-security threats and practices.

Also, various defense strategies to prevent issues related to the integrity and privacy of data have been incorporated in this study. Then we studied cyber-security defense strategies for organizations and institutions. We learned about information security policies and their implementation. We also learned the importance of these policies in the prevention of attacks in cyberspace. We learned about the various aspects of policy implementation in terms of environmental and physical safety.

Then we studied various practices and methods an organization must implement keeping the provision of cyber-security training and certifications. Then we examined various end-user security vulnerabilities and threats like ransomware, phishing attacks, and insecure public internet connections. In the final section, we examined various challenges that are being faced by the industry due to cyber-threats and related activities. At last, we provided some next steps to be taken into account relating to the security and threat prevention in industry 4.0.

**The attack in industry 4.0**

Industry 4.0 is a system architecture in which intelligent systems are used to carry out different processes. It is based on virtualization, real-time, autonomous management, and modularity principles [13].

The sources of the attacks need to be identified and their defense strategies should be developed against cyber-attacks. The attacks are mainly targeted on IoT and CPS [14].

**The Cyber-Physical Systems**

The ecosystem is interconnected with the internet and the physical world through Cyber-Physical Systems, in industry 4.0. The CPS has devices that communicate with the physical world as well as interact with each other [15]. CPS applications are found in robotics, medical devices, and manufacturing systems [16].

The data sources in CPS are the sensors and production systems. The CPS also has a cyber architecture that acts as its information centre [15]. In CPS, the machine situations are examined, data is analyzed and decisions are taken. Finally, feedback is provided, and reconfiguring of the machines is done. Preventive and corrective decisions are taken [17].

**Internet of Things (IoT)**

The real-time communication and management of sensors and control systems are called the Internet of Things [18]. There are 3 layers in the IoT architecture. These are detection, application, and communication layers [19]. Table 1 shows the risks and threats in layers of IoT systems[20]:

Table 1. Risks and threats

| IoT Layer | Security Threats |
|---|---|
| Physical | Tampering, Denial of Service |
| Networking | Passive Monitoring, Eavesdropping |
| Application | Integrity, Modifications |

About 10 percent of the total IoT devices work on the internet. There is a rapid pace in the use of IoT devices. The problem is that this growth brings various vulnerabilities that make these devices less secured [21].

**Cyber-security**

The protection of privacy and security due to specific risks and vulnerabilities generated by cyber-attacks is called cyber-security. Cyber-security priority is to defend the integrity, accessibility, and data privacy [22]. The aim of cyber-attacks is service blocking, unauthorized access to data, disclosure, sharing, and destruction. Cyber-attacks are grouped into [23]:

- Vulnerability and Penetration Test
- Sniffing
- Phishing
- E-mail spam
- Malicious software: Virus, Adware, Trojan, Worm, Spyware

**. Cyber-security defense strategiesfor Corporations**

Institutions that plan to install industry 4.0 structures should take preventive measures against the attacks that lead to issues regarding accessibility, integrity, and privacy [24]. These attacks are divided into two main categories which are nature-induced and human-induced threats [25]. External threats include activities such as

theft or espionage due to unauthorized access to the cyberspace [26].

The risk from cyber-attacks is an important consideration for the institutions that have implemented the Industry 4.0 architecture. The companies should identify the vulnerabilities and how to take preventions against them. The next section explains the preventions to be taken by institutions to protect their data and cyberspace.

**Information Security Policies**

The corporations that install industry 4.0 infrastructure should implement information security policies. The ISO/IEC 27001 as well as the ISO/IEC 27002 standards should be taken into account while implementing the information security policies. Information security management and processes are defined by the ISO/IEC 27001 standard, whereas the security preventions of the 27001 process are defined by the ISO/IEC 27002 standard. While implementing the information security policies, the following headings under integrity, privacy, and accessibility should be included:

- Environmental and physical safety
- Communication security
- Access control
- Use of cryptographic controls
- Protection from malicious software

**Control Systems Protocol vulnerabilities**

Several protocols for communication are used in control systems of various industries. They are categorized into open systems and closed systems. The communication between manufacturer-independent devices is observed in open system communication protocols whereas the communication between the manufacturer's own devices is observed in closed system communication protocols.

Remote monitoring as well as control of large-scale systems is facilitated by Supervisory Control and Data Acquisition, (SCADA). The SCADA systems help in managing production processes as well as their monitoring. Insecurity standards of SCADA systems, the API 1164 was the first published security protocol. The Profinet, DNP3, and Modbus are commonly used protocols.

**Staff Training**

The critical prevention here should be done by the IT managers of the corporation. They need to know about the source as well as the attack target. Technical personnel and system administrators should provide cyber-security training, periodically. Many organizations/institutions provide cyber-security training. The security staff must participate in cyber-security certifications and training, in corporations. They must learn to take preventions by using the techniques and tools for cyber-attacks. The certifications used for cyber-security which have international validity are as follows:

- GPEN
- Council Certified Network Defender
- ISO 27001
- Council Certified Ethical Hacker

**End-User Attacks and Defence Strategies**

Although industries and corporations are incorporated in industry 4.0, the end-users form an essential part In its network. The end-users should know the precautions and how to implement them in-home and outdoor environments.

**Ransomware**

They are a type of viruses that can infect computers and in turn demand some money from victims. They encrypt the files stored on infected computers and ask the users for money to decode the files again [27]. It can infect in the following ways:

- Social Engineering
- Harmful Advertising
- Exploit Kits
- Drive-by Downloads

**Public connections**

Network services are generally available in hotels, cafes, and outdoor settings. One of the biggest threats is that the user and the attacker are in the same network. The preventions for cyber-attacks in internet networks with password-free connections are as follows:

**SSL web pages**:They offer the most secure operation. If any website has SSL security, its address starts with an "https://" tag. Always use the "HTTPS" on websites where login information is required. Despite secure connections over the https, it is recommended not to access accounts such as the university, bank, government, and organization.

**VPN (Virtual Private Network):**These are powerful preventions taken in public wireless network connections to provide an encrypted and secure connection. These connections can be created on iPhone/Windows/Android and other operating systems by installing the required software.

**Password stealing attacks**

The attacker generally uses a variety of methods to steal passwords. They vary from connected networks to the method of attacks. Methods such as phishing attacks and social engineering are preferred to steal passwords of the users.

**Phishing Attack:**In this method, the users are made to log into fake sites by spoofing the sites of their organizations or institutions. In this attack, the user is sent a link in the e-mail and asked to click on it to sign in to the fake site. All the e-mail account users are vulnerable to phishing attacks.

Access to pages directed from e-mail should not be provided to avoid phishing attacks. Spam emails must not be responded to. Another prevention to be taken is to use a spam filtering feature with security software.

**Social Engineering:** In it, the user is defrauded by the attacker with a specific scenario. In social engineering, the attacker uses his abilities to convince the user. When social engineering attacks are examined, different techniques are applied [28]. These are:

- Fake sites or pages
- Counterfeit product and service

- Phone
- Trojans
- Garbage mixing

A skeptical attitude must be shown in social engineering attacks.

**Challenges**

The various challenges that are being faced by industry 4.0 due to cyber-attacks are:

- Decreased production, miscommunication in devices, data loss, and disruption in services. These are mainly accounted for the challenges in the industry 4.0.

- Industry 4.0 uses IoT devices that are vulnerable to cyber-attacks and therefore it makes the whole system vulnerable since the coordination and communication between devices are affected adversely.

- It also consists of modern cyber architecture or the Cyber-physical systems that account for most of its infrastructure. The CPS is not risk proof and may encounter various infections due to cyber-attacks. This can cause the whole system to work abruptly and may even lead to a system shutdown.

Therefore, various cyber-security defense strategies have been proposed and should be implemented to incur minimum losses due to cyber-attacks.

**Next steps**

- The organizations and end-users have been advised to examine various cyber-security risks and vulnerabilities of their systems. At the same time, they have been advised to incorporate cyber-security preventions and strategies.

- The information security policies that are formulated for cyber-security precautions must be taken into account by the organizations.

- The organizations must also train their staff for these vulnerabilities and how to cope with them by providing training and certifications in cyber-security.

- The end-users have been advised not to access unknown email links which redirect them to fake sites resulting in data breaching of sensitive data or some information that is highly confidential.

**Conclusion**

In this study, various defense strategies that must be taken by corporations and end-users towards the cyber threats in industry 4.0 are discussed and explained. At first, the sources of attacks are identified and then defensive strategies against these threats are determined. Secondly, the solutions to prevent these attacks were provided. The corporate encounter difficulties like the security of their IoT devices, staff training as well as non-effective usage of the network and its assets. In the end-user dimension, we have examined the lack of security software and strong passwords. Finally, corporations are advised to implement cyber-attack preventions more carefully. An intensive process needs to be carried out for the implementation of the study results.

**References**

1. Lasi, Heiner, Peter Fettke, Hans-Georg Kemper, Thomas Feld, and Michael Hoffmann. "Industry 4.0." Business & information systems engineering 6, no. 4 (2014): 239-242.

2. J. Lee, B. Bagheri, and H.A. Kao, A Cyber-Physical systems architecture for industry 4.0-based manufacturing systems, Manufacturing Letters, 3, 18-23, 2015.

3. Y. Lu. Industry 4.0: A survey on technologies, applications, and open research issues, Journal of Industrial Information Integration, 6, 1-10, 2017.

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

5. N. Jazdi. Cyber-physical systems in the context of Industry 4.0, In Automation, Quality and Testing, Robotics, 2014 IEEE International Conference, 1-4, 2014.

6. J. Lee, B. Bagheri, and C. Jin, Introduction to cyber manufacturing, Manufacturing Letters, 8, 11-15, 2016.

7. D. F. Hsu, D. Marinucci, and J. M. Voas, Cybersecurity: Toward a secure and sustainable cyber ecosystem, Computer, (4), 12-14, 2015.

8. L. J.Wells, J. A. Camelio, C. B. Williams, and J. White, Cyber-physical security challenges in manufacturing systems, Manufacturing Letters, 2(2), 74- 77, 2014.

9. G. P. Gupta, M. Kulariya, A framework for fast and efficient cybersecurity network intrusion detection using apache spark, Procedia Computer Science, 93, 824-831, 2016.

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

11. K. Kogiso, T. Fujita, Cybersecurity enhancement of networked control systems using homomorphic encryption, In 2015 54th IEEE Conference on Decision and Control (CDC), 6836-6843, 2015.

12. J. Liu, Y. Xiao, S. Li, W. Liang, and C. P. Chen, Cybersecurity and privacy issues in smart grids, IEEE Communications Surveys & Tutorials, 14(4), 981-997, 2012.

13. ] R. Y. Zhong, X. Xu, E. Klotz, and S. T. Newman, Intelligent manufacturing in the context of industry 4.0: a review, Engineering, 3(5), 616-630, 2017.

14. R. Petrasch, R. Hentschke, Process modeling for Industry 4.0 applications: Towards an Industry 4.0 process modeling language and method, In Computer Science and Software Engineering (JCSSE), 2016 13th International Joint Conference, 1-5, 2016.

15. E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui, and K. P. Chow, Security issues and challenges for the cyber-physical system, In Proceedings of the 2010 IEEE/ACM International Conference on Green Computing and Communications & International References Conference on Cyber, Physical and Social Computing, 733-738, 2010.

16. K. He, M. Jin, Cyber-Physical System for maintenance in industry 4.0, Jönköping University School of Engineering, 64, 2016.

17. B. Bagheri, S. Yang, H. Kao, J. Lee, Cyber-Physical Systems Architecture for Self-Aware Machines in Industry 4.0 Environment, IFAC-Papers Online, 48-3 1622–1627, 2015.

I. Lee, K. Lee, The Internet of Things (IoT): Applications, investments, and challenges for enterprises, Business Horizons, 58(4), 431-440, 2015.

18. ] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, Future generation computer systems, 29(7), 1645-1660, 2013.

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

20. D. Pancaroğlu, 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, 2018.

21. R. Von Solms, N. J. Van, From information security to cybersecurity, computers & security, 38, 97-102, 2013.

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

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

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

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

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

27. K. Krombholz, H. Hobel, M. Huber, and E. Weippl, Advanced social engineering attacks, Journal of Information Security and applications, 22, 113-122, 2015.