Research Article

Industry 4.0 and Cyber Security Issues and Challenges

Mamoona Humayun[a], NZ Jhanjhi[b,*] ,Muhammad Nabil Talib[C], M H Shah[d], G. Sussendran[e]

[a]Department of Information Systems, College of Computer and Information Sciences, Jouf University, Al-Jouf, Saudi Arabia
[b]School of Computer Science and Engineering (SCE), Taylor's University, Selangor, Malaysia
[c]Papua New Guinea University of Technology, Lae, PNG
[d]Department Of Communication and Media Studies, University Of Sargodha, Sargodha
[e]Department of Information Technology, Vels Institute of Science, Technology and Advanced Studies, Chennai, India;

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract : In the current era of technology, by exploiting the vulnerabilities of networked production equipment, a growing number of cybersecurity breaches have adversely affected business efficiency especially in the context of Industry 4.0. Or Industrial internet of things (IIoT). Cyber-attacks on sensitive industrial equipment may disrupt the corporate business model in some cases. Therefore, there is a need to provide an awareness to the industry 4.0 practitioners about the layered architecture of Industry 4.0 along with possible attacks targeting these layers. Further, the consequences of these attacks along with countermeasures will provide a better overview of the situation. It will also help Industry 4.0 practitioners in better management of the cyber physical system. To do this, this paper provides a detailed overview of possible cyber-attacks targeting each layer of industry 4.0 along with the consequences of these attacks and corresponding countermeasures. Further, a layered framework is provided as a contribution to research that will provide end-to-end protection from existing cyber-attacks.

Keywords: Industry 4.0, Cyber-security; industrial internet of things (IIoT); cyber-physical system; vulnerabilities

1. Introduction

To meet today's diverse and dynamic market demands, companies around the globe are in the midst of transformation. A new wave,' Industry 4.0', has arisen in a current scenario of technological innovation happening every day. In 2011, the word 'Industry 4.0' or 'Industrial Revolution 4.0' emerged from a project within the German government's high-tech policy to encourage the computerization of production. Currently, the advancement of IoT devices has made risen the phenomenon of industry 4.0. Three critical phases are included in Industry 4.0: First, digital records are collected by sensors attached to industrial assets, which capture data by closely imitating human feelings and thoughts. This technology is known as the fusion of sensors. Second, the analyzing and visualizing phase involves the implementation of analytical capabilities with sensors on the captured data. Many different operations are done with background operations, from signal processing to optimization, visualization, cognitive and high-performance computing. To help with the enormous amount of data, an industrial cloud supports the serving method. Thirdly, turning the aggregated data into concrete results, such as additive manufacturing, autonomous robots, digital design and simulation, is the stage of transforming ideas into action. Raw data is stored in an industrial cloud with data analytics software and then converted into technically functional information.

In the globally interconnected digital world, threats to the IT infrastructure are also rising. Therefore, as the industry continues to expand and leverage the growing computing power available to customers through smartphones and laptops, certain steps need to be taken to ensure safe and secure transactions. The central concern that all governments and business organizations follow at the highest level of priority is cybersecurity. It is a defense against violence, unauthorized access, and theft of business information and precious knowledge about a topic or system in digital form. Before finding a solution to cybersecurity breaches, there is a need to synthesize the existing knowledge on possible cybersecurity threats targeting various layers of IIoT along with consequences and countermeasures. To fill this gap, upcoming sections will provide a broader overview of the existing cybersecurity challenges of IIoT, the impact of these security threats on industry 4.0, and countermeasures that need to be taken for mitigating the risk of cyber threats. The remaining paper is organized as: section two will provide a detailed overview of cybersecurity challenges targeting various layers of IIoT. Section 3 will propose a framework for providing end-to-end security of IIOT. Section 4 will conclude the paper by providing directions for future work.

2. Cyber Security and Industry 4.0

The basic industry 4.0/IIoT architecture consists of 4 layers namely; the sensing layer, network layer, service/data layer, and application layer. Below we describe the core functionality of each layer. Cybersecurity threats faced by each layer, consequences of these attacks, and countermeasures.

2.1. Cyber-attacks targeting Sensing Layer of IIoT

The IIoT sensing layer is vulnerable to direct physical access and is the target of the following types of attacks

2.1.1. Tampering

In this attack, an attacker physically modifies the devices or communication link. Hardware devices can be identified, credentials can be stolen or replaced [1]. In IIoT, interconnected devices might be deployed at remote locations and are usually left unattended, an attacker can take the benefit of the situation and can extract secrets, modify information and replace them with malicious nodes. This attack can also be performed by altering the data while it is getting transmitted from source to destination [2-4].

Consequences of Tampering

Tampering attack violates the confidentiality, integrity, and availability of the systems

Countermeasures

Tamper-resistant packaging is a way of avoiding tampering attacks however it is an expensive solution. Some other defense mechanisms involve tamper-proofing and hiding [5-7].

2.1.2. Denial of Service (DoS)

IIoT devices usually communicate via radio access technology at the physical layer level. This wireless link is vulnerable to DoS attack, which can be done either through jamming or in the form of signal distortion [8-15].

Consequences of DoS

This attack may compromise system availability to the intended users.

Countermeasures

There exist no general solution to this problem, however; the spread spectrum technique can be used to protect against jamming. One possible solution may be monitoring and traffic interpretation, but this solution usually works at higher layers of IIoT [8, 9, 11-15].

2.1.3. Sensors as Security Treats

IIoT sensors can also be a source of cyber-attack. If sensors are deployed carelessly, it can be a source of distributed DoS attacks. This type of attack doesn’t need any complicated tool to access sensors. Further, these types of attacks are becoming more prevalent due to easy access to the sensors and limited security measures [16-18].

Consequences of Sensors as security threats

If a sensor is exposed to an attacker, the attacker can transfer malicious code or may trigger a message to activate malware on IoT devices, sensitive data may be captured or even encrypted information can be extracted along with decryption keys [16, 19-22].

Countermeasures

Security threats related to sensors can be eliminated in different ways including enhancing sensor management system, protecting sensed data, using public-key encryption to secure sensor data, intrusion mechanism should be adopted and data sharing among sensors should be done in a controlled way [8, 23-26]. Figure 1 provides an verview of cyber-attacks targeting the physical layer of IIoT along with possible causes/consequences of these attacks

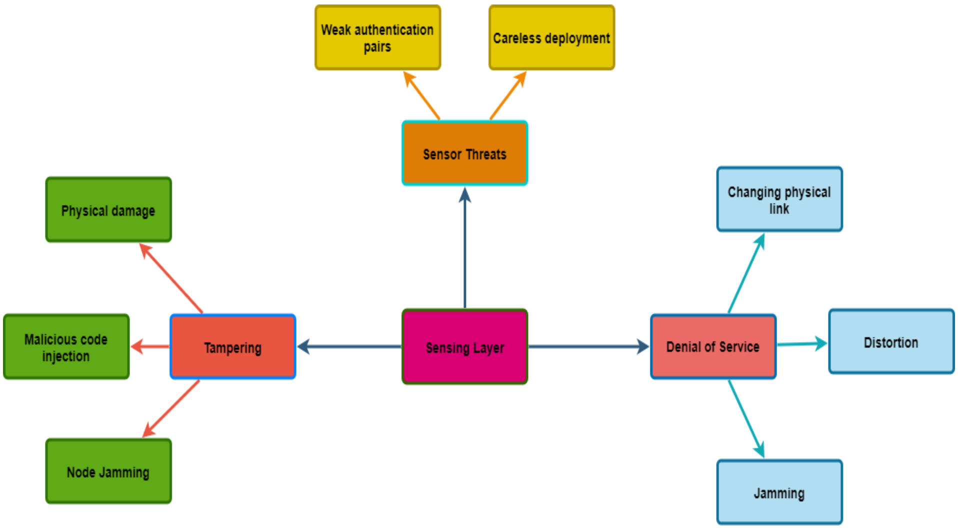

Fig. 1: Cyber-attacks targeting sensing layer of IIoT

2.2. Cyber-attacks targeting Network Layer of IIoT

In this subsection, we will discuss possible cyber-attacks targeting the network layer of IIoT

2.2.1. Denial of service (DoS)

There exist various DoS attacks that target the network layer of IIoT. In a DoS attack, network resources become inaccessible to its intended user. Figure 2 shows an overview of the DoS attack.

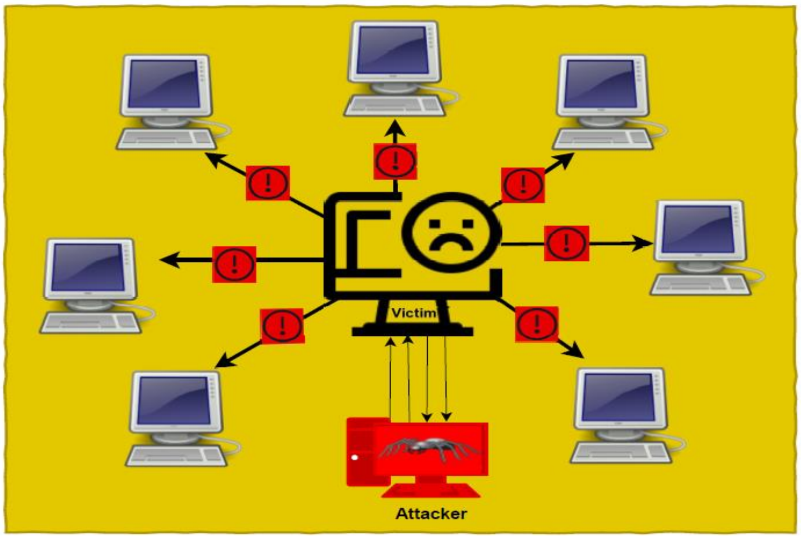

Fig. 2: How DoS Attack works

Below we describe the possible reasons and subtypes of DoS attack

Exhaustion. Network resources such as buffers, throughput, and computation capacity may be exhausted by targeting the resource of any network node[27, 28].

Collision: It is a type of jamming attack in which attackers decrease the throughput of the network or sometimes make communication impossible. It is in the form of electromagnetic interference using frequency band wireless signals [29, 30].

Spoofing: it involves satirizing a user program to gain unauthorized access. It is usually performed by sending malicious information from an unknown source. In spoofing, the attacker plays a dual role; as a user and as a router, and the actual user is unaware of what is happening [11, 26].

Sinkhole attack: Sinkhole are the nodes that are compromised. In this attack, while data is transferring from source to destination, when the data reaches the compromised node/sinkhole node, it is altered or forwarded to a wrong destination. In this attack, compromised node attract network traffic by advertising fake routing update. Sinkhole attack can also be used to launch other attacks on network including, spoofing attack and selective forwarding attack [31-34].

Unfairness: It involves the corrupting fairness mechanism of wireless sensor networks (WSNs). It exhausts WSNs by sending heavy traffic or causing repeated collision [35-38]

Selective forwarding: In this type of DoS attack, a compromised node may receive and alter data by dropping some messages and forwarding selected messages. As a result of selective forwarding, the host will not receive complete information or sometimes will receive corrupted information [34, 39-41].

Wormhole attack: Wormhole attack is considered a high severity attack in which a tunnel is established between two nodes and packet is forwarded among each other. These malicious nodes pretend that they are very close to each other so that other nodes could send packet through these nodes [34, 42-44].

Sybil attack: Sybil attack is one of the emerging attacks targeting IIoT. In this attack, the attacker uses multiple fake identities or abuse pseudo identities and thus compromise the effectiveness of the system. Figure 3 shows the working of Sybil attack. A lot of Sybil attacks are reported on social media where attackers use multiple identities to spread spam and advertisement Sybil attacks generate spam while sometimes attackers broadcast malware and phishing websites to steal users' private information. Further, several Sybil attackers behave like a normal user, therefore it is difficult to detect that an account is Sybil or not [34, 45-47].

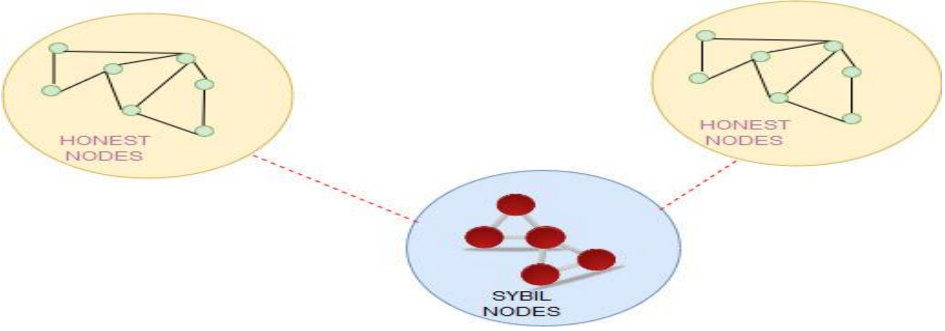

Fig. 3: Sybil Attacks

Flooding: Network flooding and DDoS flooding involve sending a large amount of traffic or service requests to the target system to exhaust network resources. As a result of heavy traffic, the target system sometimes becomes usable or even crashes in some cases [32, 34, 48-50]

Node Replication: In this type of attack, the attacker copies the identity of a node and use the same identity to send false data to disrupt the network [25, 28, 51].

Consequences of DoS threats

Collision attack may cause a loss of data availability [29, 30, 52]. Spoofing attacks cause a loss of data integrity and confidentiality [11, 26]. Sinkhole attacks may cause tamper of data, damaging the regular traffic of the network and sometimes it challenges network security [31-34]. Unfairness may interrupt the availability, integrity, and confidentiality of a wireless network that is a part of IIoT [35-38]. Selective forwarding causes loss of data. Sometimes, incomplete or altered information reaches a destination that is more dangerous than the loss of information [34, 39-41]. Packet transmission takes more time in case of wormhole attack [34, 42-44]. The presence of Sybil attacks in the IIoT context causes many problems including wrong report generation, loss of privacy, and spam received [34, 45-47]. Most of the flooding attacks try to make the victims' services unavailable thus leading to loss of revenue, resource wastage, and increased cost of service restore [32, 34, 48-50]

Countermeasures

A jamming attack can be minimized through antijamming, active jamming, and faraday cages. Spoofing can be avoided using identity-based authentication, IP security, key distribution, and digital signature [53]. Sinkhole attacks may be avoided by implementing an intrusion detection system (IDS), using rule-based technology to make aware the compromised node about the existing attack, use link quality indicator to monitor individual nodes, and use mobile agent to defend nodes [25, 54]. Unfairness may be avoided by providing a proper security mechanism or using an algorithm for WSNs security[25]. Selective forwarding may be reduced by monitoring neighbor nodes, introducing an attack detection mechanism, controlling packet collection and analysis of alternate path [28, 55, 56]. Wormhole attacks can be monitored and controlled using IDs, neighbor validation, and distance calculation[57]. Sybil attack may be monitored and controlled using cryptography, profile matching, behavior classification, channel estimation, and by monitoring users' mobility [58, 59]. Packet marking, packet tracing, and link testing can be used to avoid flooding [16, 60].

2.2.2. Man-in-the-Middle attacks

This kind of attack occurs when an attacker gains information access during the information transmission between sender and receiver as shown in Figure 4. Following three attacks belong to the category of Man-in-the-Middle attack

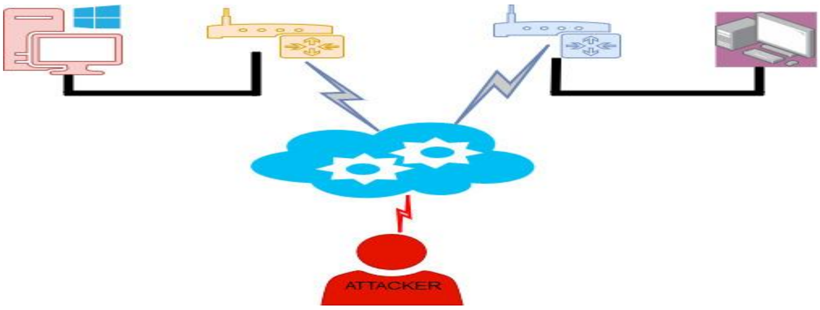

Fig. 4: Man-in-the-middle attack

Eavesdropping: It is a common type of spoofing in which an attacker intercepts communication between two points. In this attack, the attacker uses a specialized program to sniff and records data packets during communication and listen or read the data using cryptographic tools for decryption[61, 62].

Routing attack: In this attack, the attacker changes the routing information and thus create a routing loop to decline the quality of service [32, 34, 39]

Replay attack: In this attack, an attacker captures a signed packet and try to decrypt it, if it is not possible to decrypt it then retransmit it at a later time [21, 63, 64].

Consequences of Man-in-the-Middle attacks

Eavesdropping attacks cause a loss of data availability, integrity, and confidentiality. Routing attack deteriorates the quality of service by intercepting routing path. Replay attack causes an alteration in data packets and makes unauthorized access of these data packets easy [180, 181, 183]

Countermeasures

Eavesdropping attacks can be minimized using two techniques; firstly by adding a semi-dynamic controller signature into LLDP packets to ensure the integrity of packets. The second way of protecting IIoT from eavesdropping attack is to detect and block fake links by comparing node to node communication time with a predefined threshold value[34, 65]. Routing information needs to be protected using encryption. Replay attacks can be prevented using the message authentication code and message sequence number. Further, the timestamp mechanism is also used to prevent replay attacks [21, 63-65]. Figure 5 describes the key network layer attacks along with sub attacks

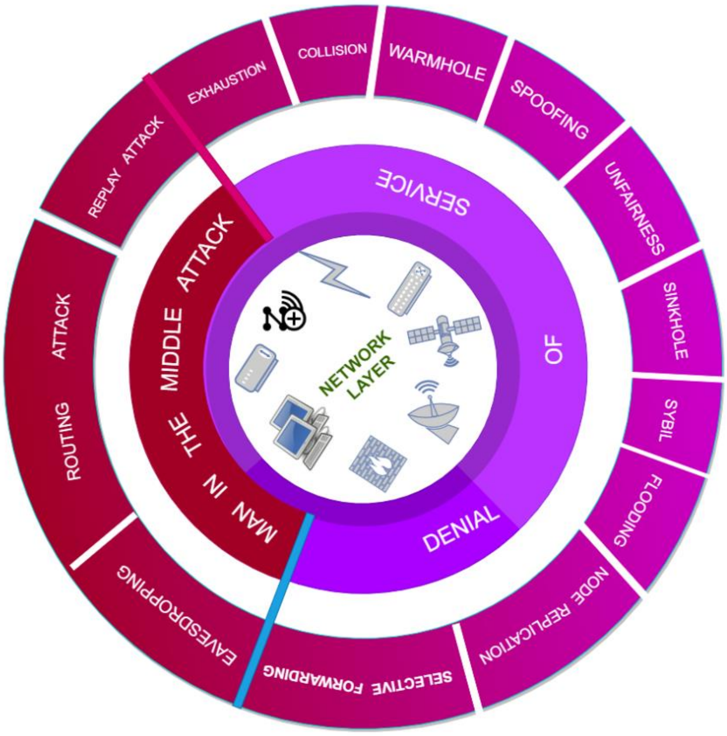

Fig. 5: Cyber-attacks targeting network layer of IIoT

2.3. Cyber-attacks targeting Service/data processing Layer of IIoT

In the industry 4.0 context; data aggregation and processing are usually done on the data processing layer where usually, data is stored in the cloud. This layer is the target of various types of attacks from the end nodes including malware, Exhaustion, eavesdropping, DoS, network intrusion, logon abuse, fragmentation attack, session hijacking, malicious insider, and the other security issues related to the cloud. Some of these attacks detail has already been discussed in previous subsections. Below we will discuss remaining cyber-attacks that target the security of the data processing layer

2.3.1. Malware

Malware is a kind of malicious software, it is specifically designed to harm the data, services, and individuals. Some examples of malware include viruses, spyware, Trojans, worms, ransomware, adware, botnets, and the like. Each malware has its way of affecting and damaging devices and data. In the IIoT context, advanced malware is also known as feature distributed malware (FDM) is a common attack at the data processing layer. In FDM, an attacker steals the target’s specific internet service account and provides harm despite highly installed security tools on the target’s system [66-70].

Consequences of Malware

Malware creates many problems: it can slow down victims’ systems, identity theft, the system may display error message continually, system crash, hijacking browser and redirecting to various sites for malicious purposes and even getting control of the systems [65-70].

Countermeasures

To protect the individual system from malware, each node must use some preventive measures like avoid opening suspicious emails, links, or websites. Antimalware software must be used to protect all network computing devices [66-72].

2.3.2. Session Hijacking

A session is created for each user when a user login any web service such as the cloud. This session keeps track of all user’s information including session ID to validate user’s requests for data. This session ends when the user logout. Usually, session data is stored in cookies or sometimes as parameters in URL. During a session hijacking attack, an attacker hijacks the session by obtaining a valid session ID and thus pretends to be an actual user and perform various malicious activities. Session hijacking attack may be active or passive: in an active attack, the attacker takes control of the victim’s machine and exchange data. In a passive session hijacking attack, an attacker monitors the traffic and discover valuable credentials [73-75].

Consequences of Session Hijacking

In the IIoT context, session hijacking can make cloud services vulnerable by breaching victim’s information. It adversely affects the integrity of the victim due to the loss of crucial information [73, 75-77].

Countermeasures

The measures used to detect and prevent session hijacking attacks include IDs, monitoring of MAC address, using SSL, HTTPS connection, educating the users, timing out session, and CAPTCHA prevention[73, 75-78].

2.3.3. Cloud Service Provider (CSP) Risks

Some of the attacks are specifically associated with data processing layers and the attacker can exploit CSP’s vulnerabilities. These attacks include back-door attacks, password guessing, social engineering, and all network-level risks that target cloud infrastructure [78-81].

Consequences of CSP risks

CSP security breaches have severe consequences including theft or loss of intellectual property, loss of data integrity, and availability and trust of the service provider [79, 80, 82, 83].

Countermeasures

To avoid the risks associated with CSP, the communication between IoT hubs and cloud management server should be encrypted. All the input to the IIoT database and application servers should be monitored to avoid malicious traffic and attacks. Cloud users should be vigilant about the risks associated with data transmission between IIoT clients and the cloud [8, 28, 79, 80].

2.3.4. Malicious insider:

This attack occurs when an insider breaches the security for getting some personal benefit or the benefits of a third party. Attacker accesses the data and uses it for malicious activities. A malicious worker can perform several attacks such as DoS, extracting confidential information, intercepting the decision-making process, and executing privileges of grant and revoke [28, 84, 85].

Consequences of insider attack

It is one of the severe attacks that harm individuals as well as organizations. It leads to several other attacks including DoS, Malware, credential loss, etc.

Countermeasures

There exist no standard measure to protect IIoT from insider threats, however; some best practices should be used to protect IIoT infrastructure from insiders’ threats. These best practices include: periodic risk assessment, security awareness training to employees, enforce separation of responsibilities and assign fewer privileges, implement strict security policies, monitor and audit employees and monitor disruptive behavior [84-88]. Figure 6 highlights the possible attacks and sub-attacks targeting the data layer of IIoT.

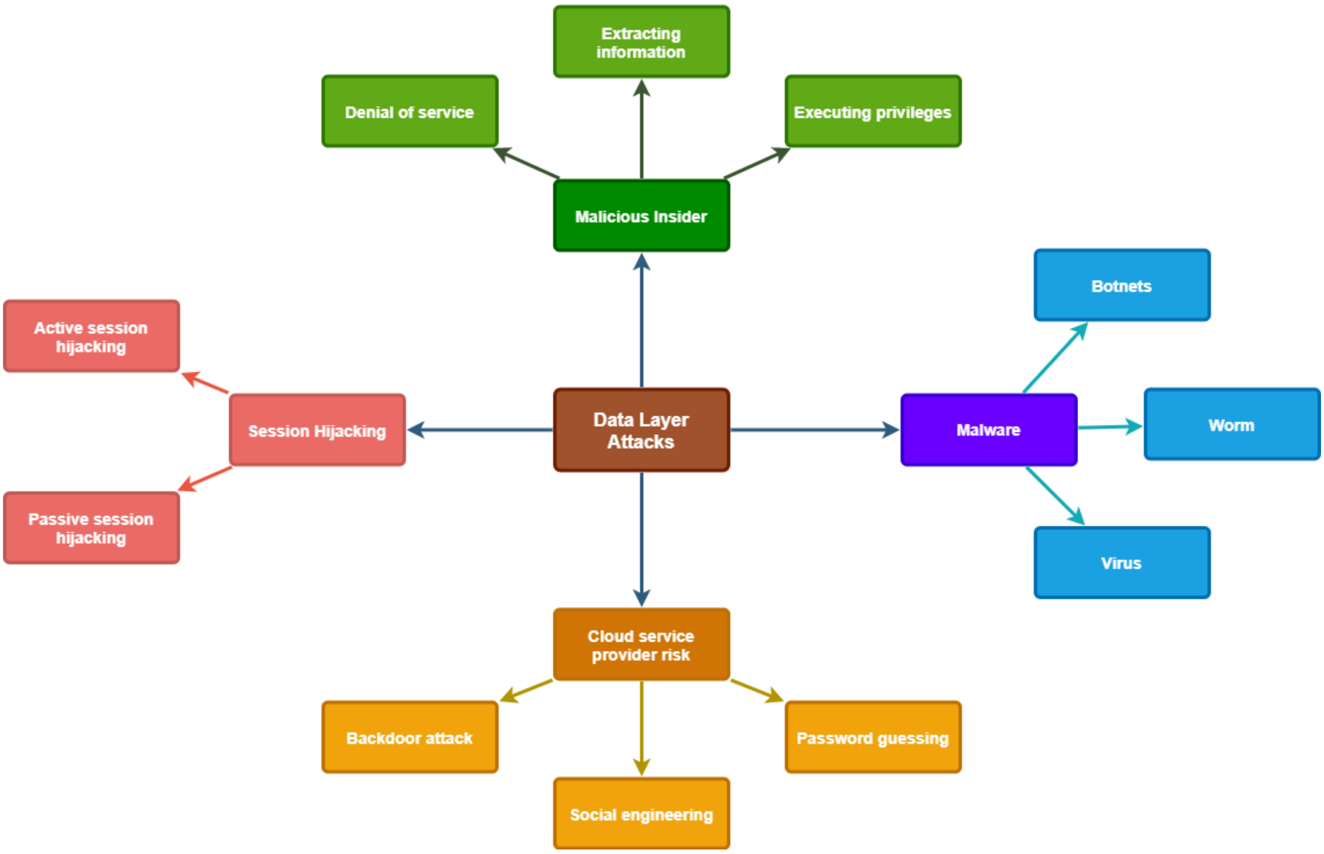

Fig. 6: Cyber-attacks targeting Data layer of IIoT

2.4. Cyber-attacks targeting Application Layer of IIoT

The application layer/interface layer is the topmost layer of IIoT that interacts with the end-user. The possible cyber threats targeting this layer include malicious code injection, DoS, phishing, and sniffing attacks. Below we will discuss those threats which have not already been addressed

2.4.1. Phishing attack

In this attack email of someone from a higher authority is hacked and used by the attacker for malicious purposes. It is one of the rapidly growing attacks in which the attacker takes the benefit of human nature and internet tricks to perform malicious activities. Phishing attacks are broadly categorized as social engineering and malware-based phishing. In social engineering phishing, attackers get access to user credentials by sending fake emails or using some fake website. On the other hand, in a malware-based phishing attack, attackers use malicious programs to hack the information [49, 89-91].

Consequences of phishing attack

Phishing attack results in theft of login information, theft of banking credentials, theft of organizational secrets, and attack propagation.

Countermeasures

The approaches used to protect IIoT from phishing include user education, authentication mechanism, network-level protection, use of client-side tools (PhishNet, Google safe browsing API, AIWL, SpoofGuard, Phishguard, CANTINA, and Phishwish) and server-side tools(TF-IDF, SVM, K-NN, DBSCAN, PHONEY, FRALEC, PILFER, robust classifier model) [49, 89-93].

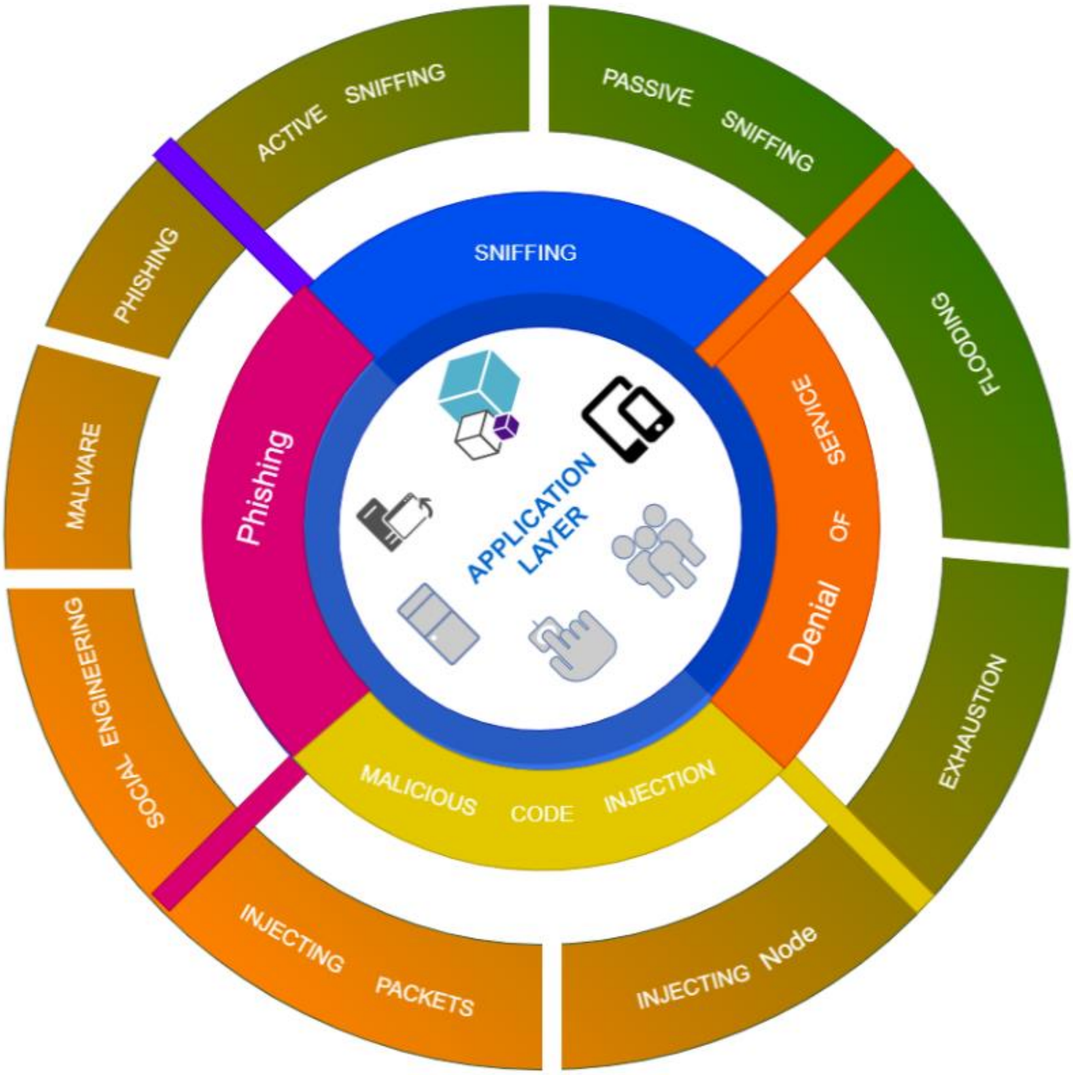

Fig. 7: Cyber-attacks targeting Application layer of IIoT

2.4.2. Sniffing attack

In this attack, the attacker uses a sniffer application for gaining network information. The attacker captures the data when it is transmitted over the network. It falls in the category of passive cyber threat because the attacker is usually invisible in this threat. It usually involves capturing unencrypted data including user credentials, transferred files, and network details, etc. Sniffing can be of different types: LAN sniffing, protocol sniffing, TCP session sniffing, web password sniffing and ARP sniffing [27, 76, 94-96].

Consequences of sniffing attack

Just like a phishing attack, a Sniffing attack also results in theft of login information, theft of banking credentials, theft of organizational secrets, and attack propagation.

Countermeasures

Some measures to avoid sniffing attacks include secure socket layer encryption especially for important transactions, use of MAC filtering, and enable WPA or WPPA 2 encryption [97-99]. Figure 7 highlights the possible attacks and sub-attacks targeting the application layer of IIoT.

2.4.3. Denial of Service

DDoS attacks on the application layer are designed to target the application itself, concentrating on particular bugs or problems, causing the application not to be able to provide content to the user. Application layer attacks are intended to target particular applications, with web servers being the most common, but any application such as SIP voice services and BGP can be used.

Consequences of DoS attack

Dos attacks create various problems such as platform become unreachable, Loss of confidential data; turnover decline, loss of productivity; and loss of business reputation.

Countermeasures

The DoS attack on the application layer can be mitigated through implementing proper firewalls and proxies, IP security, Filtering, and the use of proper authentication mechanisms.

2.4.4. Code Injection

Code injection is the manipulation of a programming error that is triggered by processing invalid data. In this attack, an attacker attempt to inject code into a compromised computer program and alter the direction of execution.

Consequences of Code Injection

Code injection is among one of the traditional and most dangerous web application attacks that can lead to data theft, loss of data, denial of service, loss of data integrity, and even sometimes total device compromise.

Countermeasures

Code injection can be prevented through input validation and sanitization, IDS, Scanning your applications, code checking, and proper authentication.

3. Proposed Framework

Section 2 has discussed possible cyber-attacks targeting various layers of IIoT. Based on the analysis of data from section 2, we have proposed a framework in Figure 8. According to the proposed framework, IIoT is divided into four layers. All these layers use different devices, protocols, and software and are vulnerable to different security attacks. The first layer of the proposed framework is the physical layer, this layer includes sensors, actuators, and other network devices. This layer is the main target of tampering, sensor threats, and DoS attacks. Tampering occurs through physical damage to the devices or malicious code injection. On the other hand sensor threats are mainly caused by careless deployment and weak authentication mechanisms. The second layer of IIoT (as mentioned in the proposed framework) is the network layer. This layer consists of two sublayers: the routing layer performing the movement of packets from the source to the destination, and the encapsulation layer forming the packets. The key attacks targeting this layer of IIoT include DoS and Man-in-the-Middle attack. Some common forms of DoS attack include jamming, exhaustion, spoofing, sinkhole, unfairness, Sybil attack, flooding, spoofing, wormhole attack, and node replication. Layer three of IIoT is Data/service layer, this layer is located between the communication HW/SW and applications and provides data transmission, storage, and connectivity services. This layer is the main target of a malicious insider, CSP attacks, malware, and session hijacking. Malicious insider attacks may be launched via extracting information, DoS, and privileges execution. Industry 4.0 uses cloud services for data storage and transmission, therefore, it is a victim of CSP attacks. Some common CSP attacks targeting the service/data layer of IIoT include backdoor attack, social engineering, and password guessing. Malware attack at this layer is launched in the form of virus, worms, and botnets while session hijacking in which attackers hijack users' session actively or passively. The fourth layer of IIoT is the application layer, this layer is responsible for the provision of services and specifies the collection of protocols for messages exchanged at this level. This layer is the main target of phishing, sniffing, code injection, and DoS attacks. Phishing attacks at this layer come either in form of malware or through social engineering. Sniffing attacks both in active mode and passive mode target this layer by capturing network traffic using a sniffer. DoS attack at this layer mainly targets via exhaustion and flooding. Last but not the least is code injection attack, this attack target network node as well as network packets.

The proposed framework mentions possible attacks targeting IIoT layers. The role of IIoT researchers and practitioners is not only to make IIoT users aware of it but rather they should also try to find more resilient solutions to these attacks for leveraging the maximum potential of IIoT.

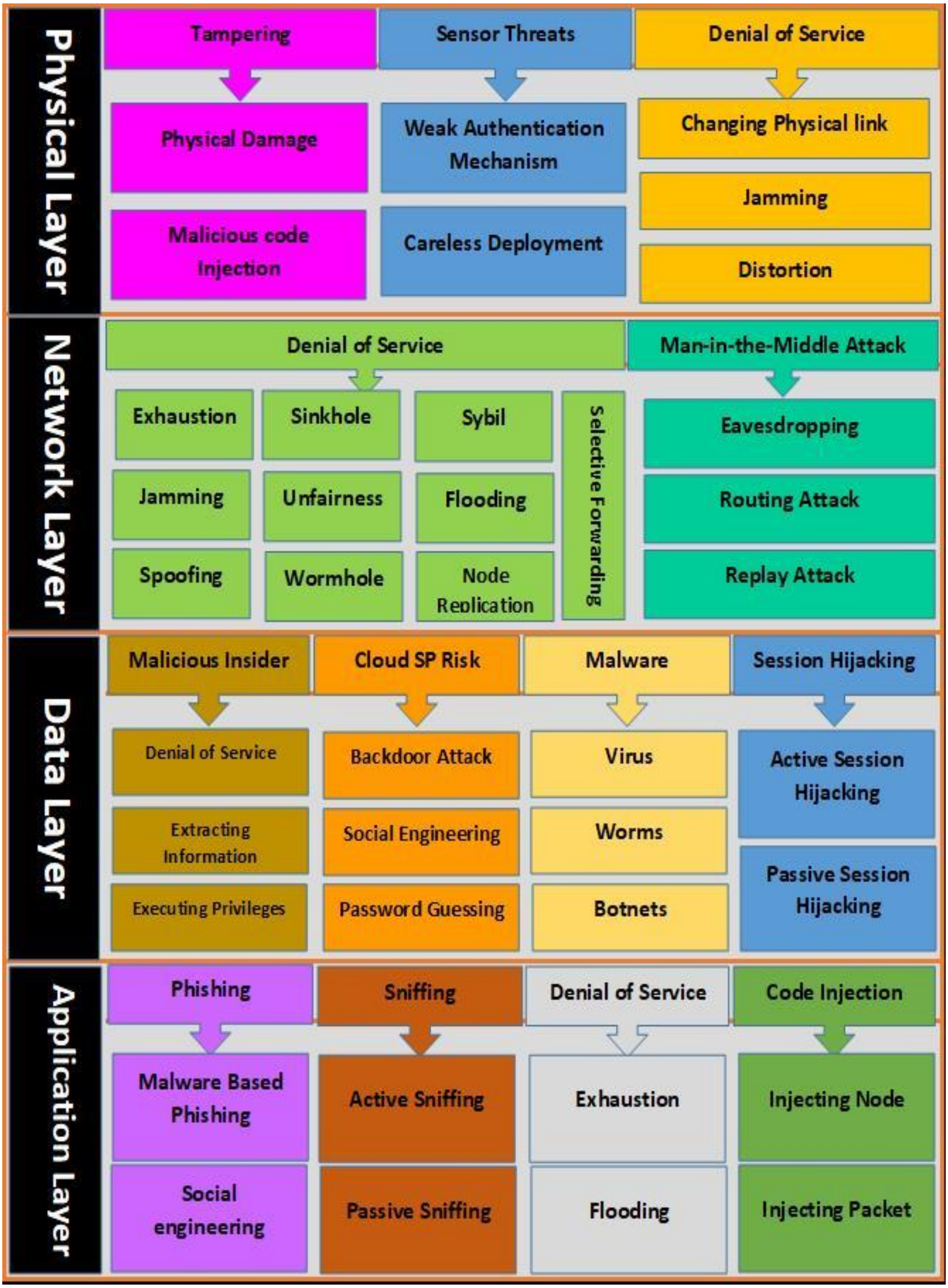

Fig. 8: Proposed Framework

4. Conclusion and Future work

(IIoT) refers to interconnected sensors, tools, and other devices that are interconnected with industrial computer applications, including manufacturing and energy management. This connectivity facilitates the collection, distribution, and review of data, potentially promoting productivity and performance improvements, and other economic benefits. Despite the highly positive role of IIoT as a key pillar of industry 4.0, it is facing the problem of cybersecurity breaches. Various studies have discussed the cybersecurity challenges faced by I4.0, however, these studies mainly discuss I4.0 challenges in general. Further, existing studies mainly target specific challenges. In this paper, we have synthesized the literature on cybersecurity challenges for IIoT that is one of the key pillars of I4.0. To do this, first, we defined the layered architecture of IIoT, then we identified the possible security challenges targeting each layer of IIoT along with its consequences and countermeasures. As a contribution to research, we have proposed a framework that provides an overview of these challenges. The proposed research is helpful for I4.0 practitioners and researchers in getting in-depth awareness about cybersecurity breaches and their mitigation techniques.

In the future, we are planning to extend our work by implementing the proposed framework in real-time I4.0 settings.

References

1. Stellios, I., et al., A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Communications Surveys & Tutorials, 2018. **20**(4): p. 3453-3495.
2. Zulkipli, N.H.N., A. Alenezi, and G.B. Wills. IoT forensic: bridging the challenges in digital forensic and the Internet of Things. in International Conference on Internet of Things, Big Data and Security. 2017. SCITEPRESS.
3. Pan, Y., et al., Taxonomies for Reasoning About Cyber-physical Attacks in IoT-based Manufacturing Systems. International Journal of Interactive Multimedia & Artificial Intelligence, 2017. **4**(3).
4. Varga, P., et al. Security threats and issues in automation IoT. in 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS). 2017. IEEE.
5. Toffalini, F., et al. Careful-Packing: A Practical and Scalable Anti-Tampering Software Protection enforced by Trusted Computing. in Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy. 2019.
6. Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arabian Journal for Science and Engineering, 1-19.
7. Chen, Z., Z. Wang, and C. Jia, Semantic-integrated software watermarking with tamper-proofing. Multimedia Tools and Applications, 2018. **77**(9): p. 11159-11178.
8. Humayun, Mamoona, N. Z. Jhanjhi, Bushra Hamid, and Ghufran Ahmed. "Emerging smart logistics and transportation using IoT and blockchain." IEEE Internet of Things Magazine 3, no. 2 (2020): 58-62.
9. Lalos, A.S., et al., Secure and safe IIoT systems via machine and deep learning approaches, in Security and Quality in Cyber-Physical Systems Engineering. 2019, Springer. p. 443-470.
10. Figueroa-Lorenzo, S., J. Añorga, and S. Arrizabalaga, A Survey of IIoT Protocols: A Measure of Vulnerability Risk Analysis Based on CVSS. ACM Computing Surveys (CSUR), 2020. **53**(2): p. 1-53.
11. Du, M. and K. Wang, An SDN-enabled pseudo-honeypot strategy for distributed denial of service attacks in industrial Internet of Things. IEEE Transactions on Industrial Informatics, 2019. **16**(1): p. 648-657.
12. Yan, X., et al., Trustworthy network anomaly detection based on an adaptive learning rate and momentum in IIoT. IEEE Transactions on Industrial Informatics, 2020. **16**(9): p. 6182-6192.
13. Tajalli, S.Z., et al., DoS-Resilient Distributed Optimal Scheduling in a Fog Supporting IIoT-Based Smart Microgrid. IEEE Transactions on Industry Applications, 2020. **56**(3): p. 2968-2977.
14. Zhou, L., H. Guo, and G. Deng, A fog computing based approach to DDoS mitigation in IIoT systems. Computers & Security, 2019. **85**: p. 51-62.
15. Kim, B.-K. and Y. Kang. Abnormal Traffic Detection Mechanism for Protecting IIoT Environments. in 2018 International Conference on Information and Communication Technology Convergence (ICTC). 2018. IEEE.
16. Almusaylim, Z.A., Zaman, N. A review on smart home present state and challenges: linked to context-awareness internet of things (IoT). Wireless Netw 25, 3193–3204 (2019). https://doi.org/10.1007/s11276-018-1712-5.
17. Patel, C. and N. Doshi, Security challenges in IoT cyber world, in Security in Smart Cities: Models, Applications, and Challenges. 2019, Springer. p. 171-191.
18. Kimani, K., V. Oduol, and K. Langat, Cyber security challenges for IoT-based smart grid networks. International Journal of Critical Infrastructure Protection, 2019. **25**: p. 36-49.
19. Madhawa, S., P. Balakrishnan, and U. Arumugam, Roll forward validation based decision tree classification for detecting data integrity attacks in industrial internet of things. Journal of Intelligent & Fuzzy Systems, 2019. **36**(3): p. 2355-2366.
20. Paliwal, S., Hash-based conditional privacy preserving authentication and key exchange protocol suitable for industrial Internet of Things. IEEE Access, 2019. **7**: p. 136073-136093.

21. Li, W. and P. Wang, Two-factor authentication in industrial Internet-of-Things: Attacks, evaluation and new construction. Future Generation Computer Systems, 2019. **101**: p. 694-708.
22. Hussain, S. and S.A. Chaudhry, Comments on “Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment”. IEEE Internet of Things Journal, 2019. **6**(6): p. 10936-10940.
23. Humayun, M., N. Z. Jhanjhi, and M. Z. Alamri. "Smart Secure and Energy Efficient Scheme for E-Health Applications using IoT: A Review." International Journal of Computer Science and Network Security 20, no. 4: 55-74.
24. Almusaylim, Z.A., A. Alhumam, and N. Jhanjhi, Proposing a Secure RPL based Internet of Things Routing Protocol: A Review. Ad Hoc Networks, 2020. **101**: p. 102096.
25. Butun, I., P. Österberg, and H. Song, Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials, 2019. **22**(1): p. 616-644.
26. Khattak, H.A., et al., Perception layer security in Internet of Things. Future Generation Computer Systems, 2019. **100**: p. 144-164.
27. Lu, Y. and L. Da Xu, Internet of things (iot) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 2018. **6**(2): p. 2103-2115.
28. Berger, S., O. Bürger, and M. Röglinger, ATTACKS ON THE INDUSTRIAL INTERNET OF THINGS–DEVELOPMENT OF A MULTI-LAYER TAXONOMY. Computers & Security, 2020: p. 101790.
29. Wu, D., et al., Cybersecurity for digital manufacturing. Journal of manufacturing systems, 2018. **48**: p. 3-12.
30. Antao, L., et al. Requirements for testing and validating the industrial internet of things. in 2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW). 2018. IEEE.
31. Bhale, P., et al. Energy Efficient Approach to Detect Sinkhole Attack Using Roving IDS in 6LoWPAN Network. in International Conference on Innovations for Community Services. 2020. Springer.
32. Humayun, M., N. Z. Jhanjhi, and M. Z. Alamri. "IoT-based Secure and Energy Efficient scheme for E-health applications." Indian Journal of Science and Technology 13, no. 28 (2020): 2833-2848..
33. Zaminkar, M. and R. Fotohi, SoS-RPL: Securing Internet of Things Against Sinkhole Attack Using RPL Protocol-Based Node Rating and Ranking Mechanism. WIRELESS PERSONAL COMMUNICATIONS, 2020.
34. Qureshi, K.N., et al., A Novel and Secure Attacks Detection Framework for Smart Cities Industrial Internet of Things. Sustainable Cities and Society, 2020: p. 102343.
35. Hamid, Bushra, Nz Jhanjhi, Mamoona Humayun, Azeem Khan, and Ahmed Alsayat. "Cyber Security Issues and Challenges for Smart Cities: A survey." In 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), pp. 1-7. IEEE, 2019.
36. Gupta, B. and M. Quamara, An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. Concurrency and Computation: Practice and Experience, 2018: p. e4946.
37. Makhdoom, I., et al., Anatomy of threats to the internet of things. IEEE Communications Surveys & Tutorials, 2018. **21**(2): p. 1636-1675.
38. Wu, H., X. Lyu, and H. Tian, Online optimization of wireless powered mobile-edge computing for heterogeneous industrial internet of things. IEEE Internet of Things Journal, 2019. **6**(6): p. 9880-9892.
39. Babiceanu, R.F. and R. Seker, Cyber resilience protection for industrial internet of things: A software-defined networking approach. Computers in Industry, 2019. **104**: p. 47-58.
40. Wu, H., et al., Network slicing for conditional monitoring in the industrial internet of things. Transport, 2017. **2018**.
41. Airehrour, D., J. Ray, and S.K. Ray, A trust-aware RPL routing protocol to detect blackhole and selective forwarding attacks. 2017.
42. Mabodi, K., et al., Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication. The Journal of Supercomputing, 2020: p. 1-26.
43. Seyedi, B. and R. Fotohi, NIASHPT: a novel intelligent agent-based strategy using hello packet table (HPT) function for trust Internet of Things. The Journal of Supercomputing, 2020: p. 1-24.
44. Bostani, H. and M. Sheikhan, Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach. Computer Communications, 2017. **98**: p. 52-71.
45. Huang, J., et al., Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. IEEE Transactions on Industrial Informatics, 2019. **15**(6): p. 3680-3689.
46. Hassan, W.H., Current research on Internet of Things (IoT) security: A survey. Computer networks, 2019. **148**: p. 283-294.
47. Wang, E.K., et al., PoRX: A reputation incentive scheme for blockchain consensus of IIoT. Future Generation Computer Systems, 2020. **102**: p. 140-151.

48. Seferagić, A., et al., Survey on Wireless Technology Trade-Offs for the Industrial Internet of Things. Sensors, 2020. **20**(2): p. 488.
49. Parra, G.D.L.T., P. Rad, and K.-K.R. Choo, Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities. Journal of Network and Computer Applications, 2019. **135**: p. 32-46.
50. Wang, T., et al., MTES: An intelligent trust evaluation scheme in sensor-cloud-enabled industrial Internet of Things. IEEE Transactions on Industrial Informatics, 2019. **16**(3): p. 2054-2062.
51. Li, L., et al., A secure random key distribution scheme against node replication attacks in industrial wireless sensor systems. IEEE Transactions on Industrial Informatics, 2019. **16**(3): p. 2091-2101.
52. Hassan, M.M., et al., Increasing the Trustworthiness in the Industrial IoT Networks Through a Reliable Cyberattack Detection Model. IEEE Transactions on Industrial Informatics, 2020. **16**(9): p. 6154-6162.
53. Cho, E., et al., TwinPeaks: An approach for certificateless public key distribution for the internet and internet of things. Computer Networks, 2020: p. 107268.
54. Gautam, S.K., H. Om, and K. Dixit, Intrusion Detection System in Internet of Things, in Design Frameworks for Wireless Networks. 2020, Springer. p. 65-93.
55. Fang, W., et al., TMSRS: trust management-based secure routing scheme in industrial wireless sensor network with fog computing. Wireless Networks, 2019: p. 1-14.
56. Qadri, Y.A., et al., The limitations in the state-of-the-art counter-measures against the security threats in H-IoT. Cluster Computing, 2020: p. 1-19.
57. Deshmukh-Bhosale, S. and S.S. Sonavane, A real-time intrusion detection system for wormhole attack in the RPL based Internet of Things. Procedia Manufacturing, 2019. **32**: p. 840-847.
58. HaddadPajouh, H., et al., A survey on internet of things security: Requirements, challenges, and solutions. Internet of Things, 2019: p. 100129.
59. Pu, C., Sybil Attack in RPL-Based Internet of Things: Analysis and Defenses. IEEE Internet of Things Journal, 2020.
60. Satheesh, N., et al., Certain improvements to Location aided packet marking and DDoS attacks in internet. Journal of Engineering Science and Technology, 2020. **15**(1): p. 94-107.
61. Zhang, Y., et al., Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT. IEEE Transactions on Industrial Informatics, 2019. **15**(9): p. 5099-5108.
62. Wang, Q., et al., UAV-enabled friendly jamming scheme to secure industrial Internet of Things. Journal of Communications and Networks, 2019. **21**(5): p. 481-490.
63. Singh, J., A. Gimekar, and S. Venkatesan, An efficient lightweight authentication scheme for human-centered industrial Internet of Things. International Journal of Communication Systems, 2019: p. e4189.
64. Lara, E., et al., Lightweight authentication protocol for M2M communications of resource-constrained devices in industrial Internet of Things. Sensors, 2020. **20**(2): p. 501.
65. Saqib, M., et al., A critical review on security approaches to software-defined wireless sensor networking. International Journal of Distributed Sensor Networks, 2019. **15**(12): p. 1550147719889906.
66. Dovom, E.M., et al., Fuzzy pattern tree for edge malware detection and categorization in IoT. Journal of Systems Architecture, 2019. **97**: p. 1-7.
67. Dinakarrao, S.M.P., et al. Lightweight node-level malware detection and network-level malware confinement in iot networks. in 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE). 2019. IEEE.
68. Aman, M.N. and B. Sikdar, ATT-auth: A hybrid protocol for industrial IoT attestation with authentication. IEEE Internet of Things Journal, 2018. **5**(6): p. 5119-5131.
69. Khoda, M.E., et al., Robust Malware Defense in Industrial IoT Applications using Machine Learning with Selective Adversarial Samples. IEEE Transactions on Industry Applications, 2019.
70. Sharmeen, S., et al., Malware threats and detection for industrial mobile-IoT networks. IEEE access, 2018. **6**: p. 15941-15957.
71. Naeem, H., et al., Malware detection in industrial internet of things based on hybrid image visualization and deep learning model. Ad Hoc Networks, 2020: p. 102154.
72. Noor, M., H. Abbas, and W.B. Shahid, Countering cyber threats for industrial applications: An automated approach for malware evasion detection and analysis. Journal of Network and Computer Applications, 2018. **103**: p. 249-261.
73. Hu, Q., et al., A Session Hijacking Attack Against a Device-Assisted Physical-Layer Key Agreement. IEEE Transactions on Industrial Informatics, 2019. **16**(1): p. 691-702.
74. Humaira, F., et al., A Secure Framework for IoT Smart Home by Resolving Session Hijacking. Global Journal of Computer Science and Technology, 2020.
75. Hu, Q. and G.P. Hancke. A session hijacking attack on physical layer key generation agreement. in 2017 IEEE International Conference on Industrial Technology (ICIT). 2017. IEEE.
76. Panchal, A.C., V.M. Khadse, and P.N. Mahalle. Security issues in IIoT: A comprehensive survey of attacks on IIoT and its countermeasures. in 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN). 2018. IEEE.

77. Samaila, M.G., et al. Security threats and possible countermeasures in IoT applications covering different industry domains. in Proceedings of the 13th International Conference on Availability, Reliability and Security. 2018.
78. Baruah, B. and S. Dhal, A two-factor authentication scheme against FDM attack in IFTTT based Smart Home System. Computers & Security, 2018. **77**: p. 21-35.
79. Yu, X. and H. Guo. A Survey on IIoT Security. in 2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS). 2019. IEEE.
80. Nakamura, E.T. and S.L. Ribeiro. A privacy, security, safety, resilience and reliability focused risk assessment methodology for IIoT systems steps to build and use secure IIoT systems. in 2018 Global Internet of Things Summit (GIoTS). 2018. IEEE.
81. Humayun, Mamoona, Nz Jhanjhi, Madallah Alruwaili, Sagaya Sabestinal Amalathas, Venki Balasubramanian, and Buvana Selvaraj. "Privacy Protection and Energy Optimization for 5G-Aided Industrial Internet of Things." IEEE Access 8 (2020): 183665-183677.
82. Wang, T., et al., A unified trustworthy environment establishment based on edge computing in industrial IoT. IEEE Transactions on Industrial Informatics, 2019. **16**(9): p. 6083-6091.
83. Radanliev, P., et al., Economic impact of IoT cyber risk-analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance. 2018.
84. Al-Aqrabi, H., et al. A multi-layer security model for 5G-enabled industrial Internet of Things. in International Conference on Smart City and Informatization. 2019. Springer.
85. Khan, A.Y., et al., Malicious insider attack detection in IoTs using data analytics. IEEE Access, 2019. **8**: p. 11743-11753.
86. Raval, M.S., R. Gandhi, and S. Chaudhary, Insider threat detection: machine learning way, in Versatile Cybersecurity. 2018, Springer. p. 19-53.
87. Liu, L., Z. Ma, and W. Meng, Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks. Future Generation Computer Systems, 2019. **101**: p. 865-879.
88. Ahmed, A., et al., Malicious insiders attack in IoT based multi-cloud e-healthcare environment: a systematic literature review. Multimedia Tools and Applications, 2018. **77**(17): p. 21947-21965.
89. Lam, T. and H. Kettani. PhAttApp: A Phishing Attack Detection Application. in Proceedings of the 2019 3rd International Conference on Information System and Data Mining. 2019.
90. Mouratidis, H. and V. Diamantopoulou, A security analysis method for industrial internet of things. IEEE Transactions on Industrial Informatics, 2018. **14**(9): p. 4093-4100.
91. Xu, H., et al., A survey on industrial Internet of Things: A cyber-physical systems perspective. IEEE Access, 2018. **6**: p. 78238-78259.
92. Chuenchujit, T., A taxonomy of phishing research. 2016.
93. Gupta, B.B., et al., Fighting against phishing attacks: state of the art and future challenges. Neural Computing and Applications, 2017. **28**(12): p. 3629-3654.
94. Lezzi, M., M. Lazoi, and A. Corallo, Cybersecurity for Industry 4.0 in the current literature: A reference framework. Computers in Industry, 2018. **103**: p. 97-110.
95. Mourtzis, D., K. Angelopoulos, and V. Zogopoulos, Mapping Vulnerabilities in the Industrial Internet of Things Landscape. Procedia CIRP, 2019. **84**: p. 265-270.
96. Muna, A.-H., N. Moustafa, and E. Sitnikova, Identification of malicious activities in industrial internet of things based on deep learning models. Journal of Information Security and Applications, 2018. **41**: p. 1-11.
97. Kamble, A. and S. Bhutad. Survey on Internet of Things (IoT) security issues & solutions. in 2018 2nd International Conference on Inventive Systems and Control (ICISC). 2018. IEEE.
98. Frustaci, M., et al., Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet of things journal, 2017. **5**(4): p. 2483-2495.
99. Bhattacharjya, A., et al., CoAP—application layer connection-less lightweight protocol for the Internet of Things (IoT) and CoAP-IPSEC Security with DTLS Supporting CoAP, in Digital Twin Technologies and Smart Cities. 2020, Springer. p. 151-175.