Research Article

Overview of Cybersecurity Challenges in Fourth Industrial Revolution

Abdulrahman Abdullah Alghamdi

alghamdia@su.edu.sa,Shaqra University

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 16 April 2021

Abstract: The fourth industrial revolution (4iR) is known as Industry 4.0 and it is considered the age of innovative technologies such as mobile, social media, cloud, Internet of things (IoT), and Artificial intelligence (AI). This revolution involves a hyper connected system that includes the Internet of things and cloud computing technologies in smarter use of computers. IoT is a new standard of adopting sensors and actuators equipped within the objects for establishing an effective computing environment. With the applications of all these technological systems, cybersecurity plays an imperative role in the rise of this fourth industrial revolution security in the field of Internet of Things, Blockchain and the Artificial Intelligence. Cyber threats in the IoT such as Lack of Security and Privacy, Vulnerable to web interfaces, Vulnerable Web Interfaces and Default weak and hard coded credentials were analyzed. This research also identifies the various Cyber threats and presents a structured analysis of the most frequently adopted security applications for these attacks.

Keywords: Cybersecurity, Computer science, fourth industrial revolution, Internet of Things, Hyper connected systems, Cyber threats.

1. Introduction:

The manufacturing environment has shifted, and attackers now have unprecedented access to data, unlike in the past. In a survey, nearly 85% of respondents said they had been the victim of a cyber-attack somewhere in the world [8]. Hackers and other nation states are gaining access to secure networks, which is a source of concern. Currently, attacks on supervisory control and data acquisition (SCADA) systems have been reported across North America and Europe. Researchers conducted a survey to determine the operations methods, effects, and target sectors [9]. Basically, all incidents were labeled with the following information, which included the year of the attack. The first assault on the Power of Siberia pipeline occurred in 1982, according to the incident summary. Manufacturing has been a priority for attackers for more than two decades, as shown by this. Figure 1 depicts the past of cyber-attacks.

It is important to consider the past of previous industrial revolutions in order to comprehend the present condition of the fourth. The First Industrial Revolution took place in Britain between 1750 and 1850. This was when the theory of economic growth took hold, and specialized operation for production for national and foreign markets grew. The technical revolution is the name given to the Second Revolution. From the end of the 19th century until the beginning of the 20th century, this was the time frame. Airplanes, Henry Ford's Model T, the light bulb, and the telegram were all invented during this revolution. This time saw the introduction of mass production, which was modified by supply chain and logistics experts to allow manufacturing companies to meet supply and demand. From 1969 to 2000, the Third Industrial Revolution was underway.

Manufacturing is undergoing yet another transformation, paving the way for the systematic introduction of Cyber-Physical Systems (CPS) [9]. CPS is a network of embedded machines, physical processes, and networking that is closely linked to the Internet. This change is known as the Fourth Industrial Revolution, and it does not arrive without cybersecurity with technological implementation. Though technology has been years ahead of the laws in providing security and governance in the United States (US), the government is constantly playing catch-up [10]. Understanding the different technical structures of these connected ecosystems will help you better understand the problems that are arising as a result of this modern revolution.

2. Literature Review

Currently, almost all technologies adopt the application fourth industrial revolution based on IoT. Sensor-based wireless networks, machine-to-machine systems, big data, cloud computing, and smart apps, as well as RFID-based systems, are all used to allow the Internet of Things [7]. Manufacturing firms are very interested in the novel transition in industries, also known as Industry 4.0. With operational performance, competitiveness, and customization features, it is critical for manufacturing companies all over the world. Dealing with massive data volumes, designing human-machine interactive systems, and enhancing connectivity between the digital and physical worlds are all part of the fourth industrial revolution [8].

Fourth industrial revolution consists of three essential stages: Firstly, obtaining the digital records through sensors, which were attached to industrial assets and collects data by closely imitating the feelings and thoughts of humans. This technology is known as sensor fusion. The second stage is the visualization and analysis, which consists of an execution of the analytical properties on the obtained data using the sensors. Using the data obtained through signal processing, visualization, optimization, high-performance and cognitive computation based methods, various functionalities are done. This system is assisted by an industrial based cloud in order to assist and maintain the massive amount of data. Final process is translation of perception to activity which

includes transformation of the clustered data into required outputs. These outputs can be additive manufacturing, autonomous based simulation and digital design. In the cloud based industrial applications, raw data is computed using the applications based on data analytics and then it converts it into virtually applicable comprehension.

The extensive application of devices which were connected to each other and the services provided by them in IoT has lead various advanced forms of defense in cyber-attacks in order to make sure they are providing resilient security (Sathish Kumar and R. Patel 2014; Abomhara and Kien 2015). In the last decades, cyber threats and attacks have increased extremely. Any application or users which apply the IoT based systems are instantly or incidentally affected by this. Most of the users and applications are vulnerable to malicious attacks, which can lead to remarkable burdens in financial concern as well as innumerable losses such as the corruption of data, crashes of system, breach of privacy, reliability and market losses.

Systems which are based on the internet will be more vulnerable to the cyber-attacks on IoT during 2020 (Capgemini 2015). According to authors in [7], the total number of networked devices is projected to be 20.8 billion. By 2020, Cisco estimates that there will be 50 billion IoT links [18]. According to Huawei, the number of IoT-based connections will hit 100 billion by the year 2025. Regardless of the variations in projections, the most important finding is that significant growth is expected.

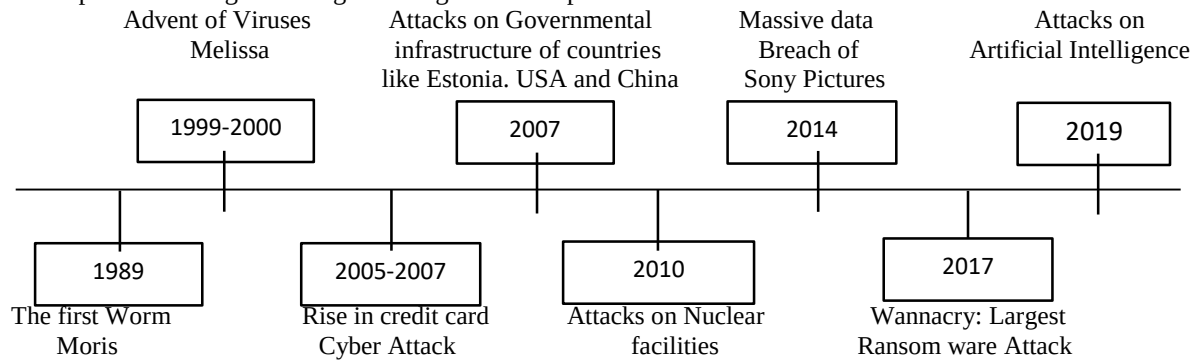

Figure 1. History of cyber-attacks

3. Internet of Things

An escalation of devices which are connected in an active network within each other is known as the Internet of Things (IoT). It is a platform where various sensors and its actuators combine continuously in order to share information [2]. An IoT system begins from the layer where a unique global identifier is used to identify the single object, which is globally identified. IoT can also be described as a system with a distinctive identifier, which is connected to the internet and is accessible in both the ways by the other systems is called as the IoT. This technology had crossed its early stages and at present, next level advanced technology is in research for the conversion of Internet into a fully integrated IoT.

IoT provides an omnipresent connectivity of internet for different types of devices, its services, and applications executed on it. These include intelligent based systems, smartphones, equipment present in offices, wireless-adapted cars, lighting and heating systems, ventilation and air-conditioning in the household etc. A device should be connected in a network if it is enabled in IoT. Various network based communication technologies such as 3G, 4G, Wi-Fi, etc. provides services of connectivity for IoT deployment on various platforms as services.

3.1. Cyber Threat in IoT Layered Architecture

The general layered architecture IoT consists of the sensor layer, layer for network, layer for processing, layer for application, and layer for business [3].

Sensor Layer:

This sensor layer is accountable for the recognition of objects and collection of information about it. RFID, barcodes based on two dimensions, and other different types of sensors are employed for the process of recognizing the object is attached to it [4, 5]. The data was gathered by these type of sensors differs based on the place, surrounding, domain, locomotion etc. These sensors can be utilized as a device to monitor the unauthorized access by an attacker.

Network Layer: This layer creates a connection between the sensor layer and the application layer. In other words, this layer is in charge of sending data obtained in the perception layer through a communication channel to other connected devices [6]. As IoT devices are attached to this layer, intruders can easily attack it.

Processing Layer: This layer is responsible for gathering and processing the data, which is sent / received from the layer of network. This layer also removes the unwanted information, which was extra in nature and also extracts the information, which is useful. Performance of the IoT can be affected by this layer when more data is received.

Application Layer: This layer uses IoT technology or defines all applications implemented to IoT. This can be applied in various applications such as the smartphones, smart homes and smart cities. Because the services provided depend on the information collected by the sensors, they may be different for each application. Different forms of threats and vulnerabilities such as the internal and external can occur when IoT devices is used in these applications.

3.2. Cyber Threats in IOT

Roman et al in [10] explained that the main challenges which should be considered in order to enhance the performance of IoT in the real world is its security. Challenges in security of IoT lists with the security objectives of the information systems such as the confidentiality of data, integrity of data, and the availability of data etc. [12]. Furthermore, there are other challenges in security such as the combination of cloud based technology and IoT exposes the platform of IoT to the cloud based vulnerabilities [13, 14].

Another significant risk may be obtained due to the substandard products and services of the IoT. These possess a potential threat and survivability to the services of IoT. For example, poor design, out-dated products proposes more risks to the applications enabled by IoT. Authors in [14] depicted that the world businesses suffer uncountable hours of time and monitory losses due to these failures, caused by poor or improper maintenance, poor and inaccurate advice from an unqualified service personnel. Furthermore, it has also been noted that the poor performance of the data entry workers and the entry of inaccurate data in the IoT devices may be accepted for information processes and critical business decisions [14].

Moreover, most of the cyber security challenges in IoT depend on the stem's built-in vulnerabilities, which reveal the infrastructure to various types of attacks. The sources may include firmware, hardware (device), system applications, data, as well as the network interfaces or ports. Also, the communication links which are bi-directional in nature established in between the objects makes the system to vulnerable attacks which are related to the network and the failure of protocol. Other related attacks include scrambling of wireless devices, intruding, trojans, attacks based on injection, and modification of the messages. For example, IP-based devices are susceptible to IP misconfiguration, which occasionally exhibits nondeterministic behavior in terms of attack. IP misconfiguration inevitably decreases reliability and performance of the system. Furthermore, the integration of IoT and cloud based computing devices covers up applications and services based on the IoT [15]. This type of integration also reveals the infrastructure of IoT and other systems to be public in networks and also in the global gateway [16].

3.3. Lack of Security and Privacy

A novel IoT based identity supported authentication methodology was proposed by Salmanet al in [16] which uses the concept of SDN on devices connected with in the IoT. SDN can be installed using fog based distributed nodes. Each device can communicate with a gateway that can support authentication. These devices are also associated with a centralized organizer which can access the central data.

Porambageet al in [17] proposed a novel pervasive based protocol for authentication purposes. They also introduced a scheme key establishment for the wireless based sensor resource networks, which are connected to the IoT based application. It is called as the PAuth Key. This Key protocol consists of two phases such as the registration phase which obtains the credentials of cryptography to various devices and its users. The second phase is the phase for authentication and also for the purpose of establishing a key in the communication of mutual entities. Zhang et al in [18] presented a novel methodology to protect against the DDoS based attacks. This can be done by assuming a network which consists of four types of nodes, which are: 1) the node for working; 2) node for monitoring; 3) node for a legitimate user; and 4) the node for attacker. Their proposed algorithm consists of various addressing nodes for the security issues of DDoS towards the network. These nodes are considered as the devices which collect all the information and run some simple tasks.

3.4. Vulnerable Web Interfaces

The most common website security vulnerabilities are as follows:

- SQL Injections
- Cross Site Scripting
- Session Management & Broken Authentication
- Insecure Direct Object References
- Security Misconfiguration
- Cross-Site Request Forgery

SQL Injections

SQL injection is one of the vulnerability in web application security where an attacker tries to use code of application in order to access or corrupt the content present in the database. If it is successful, then it allows the

attacker to create new data, read the existing data, update the existing data, modify, or delete the existing data which is stored in the database connected, which is in back-end.

Cross Site Scripting

This focuses on the user's application by inserting a code. The code can be usually a script from the client-side such as JavaScript, towards the output of web application. This methodology can be applied to change the script of the client-side in a web based application. This permits the attackers to run the scripts in the browser of the victim, which can hijack the sessions of user, deface, or redirect the websites to sites of malicious user.

3.5. Session Management & Broken Authentication

This methodology consists of various security issues, which can maintain the recognition of a user. If the credentials for authentication and the identifiers for session are not maintained, then an attacker can attack a session that is active and it also assumes the user identity.

3.6. Default weak and Hard coded Credentials

Certain switches that belong to the Netgear consist of passwords which are hard-coded in nature which permits an attacker from a remote area to validate to the web server executed on the device. This type of vulnerability influences the Netgear Switch. Once the above defined process is done, an attacked can perform the following tasks:

- Change the MAC address and serial number of the entire product
- Memory can be set manually in order to a defined value and take out that value from it
- The new firmware can be uploaded

With the type of hard-coded passwords, an admin with the default account can be created, along with a password. This password cannot be altered or disabled by other types of administrators without modifying the program manually or without software patching.

4. Blockchain:

A blockchain is the digital record of transactions. The term comes from the structure of the database, which consists of individual records called blocks that are linked together in a single list called a chain. Blockchains are used to monitor transactions involving crypto currencies and can be used for a variety of other purposes. It is decentralized in nature and provides a distributed environment for transactions, which are used to record a variety of transactions, including those involving multiple computers. Hence, any involved transactions cannot be altered without the alteration of all concurrent blocks.

The key characteristics of the blockchain include

- Decentralization
- Persistency
- Anonymity and
- Auditability

4.1. Cyber Threats in Block Chain

Nowadays, blockchain technology is increasingly receiving attention as a next-generation solution to a wide variety of transactional and recordkeeping problems.

Various threats in the block chain include:

Platform Vulnerabilities
End-User Vulnerabilities

Each application in the blockchain should be monitored by specific rules at the time of creating new data blocks. The rules include:

- Establish a set of procedures in order to verify the integrity of new data blocks before they are added to the pool of blocks.
- Apply the procedures to all the nodes that take part in the blockchain, which is called the "network of blockchain". „
- Provide methods for consensus, which are procedures for validation. These permit the participants to follow the procedure before establishing new blocks of data.

5. Artificial Intelligence

Artificial Intelligence (AI) technology is being used to help thwart the ever-present threat of a cyber-attack. Since AI applications are focused on neural networks, machine learning, deep learning, and Natural Language Processing algorithms, these machines can only behave like humans after they have been trained to perform specific tasks by analyzing large volumes of data and identifying patterns in it. As a result, AI has the ability to

make cybersecurity more effective and sensitive in the face of ever-increasing threats, as well as strengthen an organization's cybersecurity posture.

As more data and business processes migrate to the cloud, security threats have increased exponentially. Black hat hackers are persistent in their search of personal data, and as vulnerable servers fall prey to ransomware and other types of ever-evolving malware, cybersecurity has become a top priority for organizations. However, there is a ray of hope at the end of the tunnel. Organizations must begin prioritizing cybersecurity and take steps to plan not just for current but also future security threats. To reap long-term benefits from the current technological transition, sector-specific baselines and an integrated data protection system are needed.

5.1. AI based Methods Used in Cybersecurity

Following are the various types of networks that are used in the Artificial intelligence for cybersecurity [8-10].

- Deep belief Networks
- Deep Auto encoders
- Restricted Boltzmann Machines
- Deep Auto encoders Coupled with Classification Layers
- Recurrent Neural Networks
- Convolutional Neural Networks
- Generative Adversarial Networks
- Recursive Neural Networks

5. Conclusion:

This paper presents the overview cybersecurity challenges in the fourth industrial revolution. The fourth industrial revolution comprises of various innovative technologies such as mobile, sensors, cloud computing, IoT and the Artificial intelligence. Cybersecurity plays an imperative role during the rise of this digital industrial revolution, especially in the applications of all these technological systems. A detailed review is carried out on the challenges in cybersecurity in the field of Internet of Things, Blockchain and the Artificial Intelligence. Various terms such as the Lack of Security and Privacy, Vulnerable to web interfaces, Vulnerable Web Interfaces and Default weak and hard coded credentials were analyzed. This research identifies the various threats in Cyber and presents a structured analysis of the most frequently adopted applications for providing security from these attacks

References

1. Alamri, A. Ontology Middleware for Integration of IoT Healthcare Information Systems in EHR Systems. Computers 2018, 7, 51.
2. Yang, Z.; Nakajima, T. Connecting Smart Objects in IoT Architectures by Screen Remote Monitoring and Control. Computers 2018, 7, 47.
3. Burhan, M.; Rehman, R.; Khan, B.; Kim, B.S. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors 2018, 18, 2796.
4. Ali, B.; Awad, A. Cyber and physical security vulnerability assessment for IoT-based smart homes. Sensors 2018, 18, 817.
5. Heartfield, R.; Loukas, G.; Budimir, S.; Bezemskij, A.; Fontaine, J.R.; Filippoupolitis, A.; Roesch, E. A taxonomy of cyber-physical threats and impact in the smart home. Comput. Secur. 2018, 78, 398–428.
6. Butun, I.; Pereira, N.; Gidlund, M. Security Risk Analysis of LoRaWAN and Future Directions. Future Internet 2019, 11, 3.
7. Daniel S. Berman,Anna L. Buczak, Jeffrey S. Chavis, herita L. Corbett, A Survey of Deep Learning Methods for Cyber Security, Information 10(4), 2019.
8. Torres, J.M.; Comesaña, C.I.; García-Nieto, P.J. Machine learning techniques applied to cybersecurity. Int. J. Mach. Learn. Cybern. 2019, 1–14.
9. Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access 2018, 6, 35365–35381. [CrossRef]
10. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.; Du, X.; Guizani, M. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. arXiv 2018, arXiv:1807.11023
11. Abdulhammed, R.; Faezipour, M.; Abuzneid, A.; AbuMallouh, A. Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic. IEEE Sens. Lett. 2018.
12. Evans, D. L., Bond, P. J., & Bement, A. L., Jr. (2004).Standards for security categorization of federal information and information systems. Gaithersburg: U. S. Department of Commerce.
13. Pandya, D., & Patel, N. J. (2016). OWASP top 10 vulnerability analyses in government websites. International Journal of Enterprise Computing and Business Systems,6(1).
14. Pandya, D., & Patel, N. J. (2016). OWASP top 10 vulnerability analyses in government websites. International Journal of Enterprise Computing and Business Systems,6(1)

15. Samuel Tweneboah-Koduah, Knud Erik Skouby, Reza Tadayoni, Cyber Security Threats to IoT Applications and Service Domain , Wireless Personal Communications, 2017.
16. O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi,“Identity-based authentication scheme for the Internet of Things,” inProc. IEEE Symp. Comput. Commun. (ISCC), Messina, Italy, Jun. 2016, pp. 1109–1111
17. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila,“Pauthkey: A pervasive authentication protocol and key establishmentscheme for wireless sensor networks in distributed IoT applications,” inInt. J. Distrib. Sensor Netw., vol. 10, Jul. 2014, Art. no. 357430.
18. C. Zhang and R. Green, “Communication security in Internet of Thing:Preventive measure and avoid DDoS attack over IoT network,” inProc. 18th Symp. Commun. Netw. (CNS), San Diego, CA, USA, 2015,pp. 8–15.