Analysis of Cyber-Attacks in IoT-based Critical Infrastructures

Resul Daş*, Muhammed Zekeriya Gündüz**

*Department of Software Engineering, Technology Faculty, Fırat University, 23119 Elazığ, Turkey
**Department of Computer Science and Technology, Vocational School of Technical Sciences, Bingol University, 12000, Bingol, Turkey
E-mail: *rdas@firat.edu.tr, mzgunduz@bingol.edu.tr*

ORCID ID: 0000-0002-6113-4649, 0000-0003-4278-7123

Review Paper Received: 25.11.2019 Revised: 21.12.2019 Accepted: 26.12.2019

Abstract—Every country in the world has very important critical infrastructures that provide important services such as electronic communications, energy, banking and finance, critical public services, transportation and water management. Each country has different strategies for sector-based critical infrastructures. With the increase in IoT-based solutions, network and Internet connections are established in these critical infrastructures. Therefore, these critical systems included in information networks are also subject to digital attacks. It is of great importance to identify the possible types of cyber attacks, to take various precautions against these attacks and to develop protection methods. Especially today, it is vital to protect these critical infrastructures from cyber-attacks. This paper examines the attacks on critical infrastructures, especially in recent years, and presents the most common attacks. Furthermore, security approaches to mitigate or prevent IP-based cyber-attacks are mentioned.

Keywords—Internet of Things, IoT-based critical infrastructures, smart grid, cyber-attacks, cyber security.

1. Introduction

Internet of Things (IoT) is the evolution of Machine-to-Machine communication [1]. IoT make it possible to connect everything to the Internet. In addition, IoT is the connection of uniquely identifiable, embedded, computing devices that can transmit data across a network without people-to-people or people-to-machine interaction. The number of devices connected to the Internet with IoT is growing by the day. And new IoT technologies enable nearly everything can be sensed and managed on the Internet [2]. IoT is a valuable innovation but also it can be a significant cyber-security threat for critical systems. This situation is a big potential risk in terms of cyber-security, since many entry points may have security vulnerabilities. A vulnerability in the system's security chain can pose a security risk for the whole system and give opportunities to attackers. Especially, the nations' critical infrastructures must be protected from these immense cyber-security risks [3].

Due to the increasing use of IoT applications, security vulnerabilities arise. When the IoT applications are used in critical infrastructures, some serious cyber-security problems arise inherently. If cyber-attacks happen in critical infrastructures, the results would be catastrophic [4]. Shut down the power of a hospital, alter the temperatures in nuclear cooling towers, and exploit features in smart cars while they are in motion are some destructive scenarios. National critical infrastructures subject to increased cases of hacking with the aim of cyber theft, espionage, intimidation, disruption, and cyberterrorism [5]. A cyber-attack on the infrastructure of another nation may even be a potential war justification [6]. Therefore, cyber-security is a crucial topic defending a country. Cyber attacks can destroy the physical systems of an organization or nation, delegate control of these systems to an outside party, render them inoperable, or jeopardize the privacy of people's data [7].

In this article, cyber attacks for critical infrastructures are examined and, especially the studies conducted between 2008 and 2019 were examined and cyber attacks against different critical infrastructures were classified and the damages caused by these attacks to the systems were revealed. The damages to be incurred by these systems, which are of critical importance for countries, are also invaluable financially. Therefore, solutions to mitigate or prevent these attacks are discussed.

The remainder of this paper is organized as follows. In section 2, cyber-attacks against critical infrastructures and common attack types are presented. In addition, a taxonomy of recent attacks are analyzed in this section. In section 3, measures that can be taken to mitigate or prevent cyber attacks against critical infrastructures are examined. In section 4, the work is concluded.

2. Cyber-attacks to critical infrastructures

Attackers have become more capable on cyber-attacks, but most of the world's critical infrastructure systems still use legacy technologies that are vulnerable to simple cyber attacks. The growing interconnection of critical infrastructures through IoT technologies and increasing organized cyber-attacks around the world is a worrying situation. In recent years, cyber-attacks targeting SCADA control systems belonging to different critical infrastructures have been identified. Stuxnet, Havex, BlackEnergy3, and Industroyer are the most prominent ones. It is clear that the malware, which targets critical infrastructures such as water plants, gas plants, power plants, and transportation systems are professional and specially designed. A lot of IoT-based devices are integrated into the critical infrastructures for effective communication. The number of devices connected to the Internet will reach 75 billion by 2025 and this may make the situation worse [8]. However, it is possible that there will be more attacks targeting critical infrastructures in the future [9]. Major critical infrastructure sectors are shown in Figure 1. Since these critical infrastructures are developed with IoT-based solutions, they may be exposed to cyber-attacks.

2.1. An overview of recent attacks

IoT-based solutions are the most prominent technologies to improve critical infrastructures. If a device has an IP address, it means that it can connect to the Internet. It is possible to say that devices connected to the Internet are in the scope of IoT concept, thanks to the current Internet infrastructure. So, IoT devices may be exposed to nearly all cyber-attacks that may occur in IP-based environments. The security vulnerabilities of the Internet also disrupt IoT applications. Thus, this new technology comes with some cyber-security vulnerabilities. In this section, the most considerable examples of IoT-based cyber-attacks in the world and their dangers for critical infrastructures are examined.

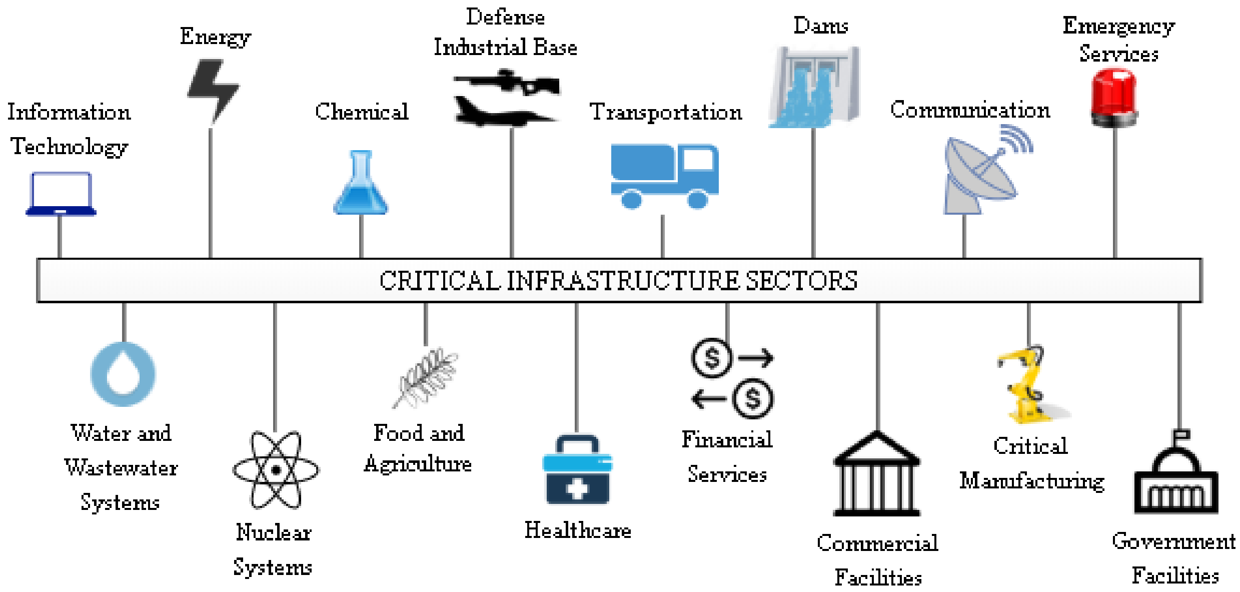

Fig. 1. Major critical infrastructure sectors

- *Tram Hacking:* A teenager hacked the tram system of Lodz city with a home-made transmitter that redirected trains. This is the first cyber-kinetic attack that injured some people [10].
- *Power Company Hacking:* An employee, fired from his company, hacked the system network to shut down the company's power forecasting systems. To do this, the attacker used his login information that was not disabled by system administrators [11].
- *Stuxnet:* It is a cyber-attack that is thought to have been carried out by the USA and Israel governments. The aim of the Stuxnet was to destroy the Iranian nuclear program by destroying uranium enrichment centrifuges at the nuclear facility. Stuxnet attacked to the SCADA systems by targeting PLCs that enable automation of electromechanical processes [12].
- *Water Distribution System Hacking:* The water distribution system at the water and sewer department was hacked. Then, the attackers presented some diagram screenshots of the system plans of water and waste-water treatment facilities. Also, three-character password was used to protect the system, and this showed that a remote attack can easily be accomplished by capturing the password [13].
- *Dam Cyber-attack:* The attackers obtained unauthorized access to the SCADA system of Bowman Avenue Dam and they were able to gather data on operations including water levels, temperatures and the status of devices. It showed that the attackers can easily change the settings of water flow, the amount of chemical used in water treatment and open the floodgates during a rainstorm. Also, the event exemplifies the immense destruction that can be caused by such a cyber-attack against IoT-based critical infrastructures [14].
- *Power Grid Hacking:* Attackers were able to seize control of Ukraine's power grid control system by hacking the SCADA system. This caused a power outage that left about 700,000 people without power for a few hours. Attackers

are thought to be testing the most complex sabotage software with this IoT-based cyber-attack [15].

- *Dyn DDoS Attack:* The DDoS attack used a system known as the Mirai botnet. Mirai botnet targets IoT devices and also scans the web to find poorly secured IoT devices that still have default usernames and passwords. Moreover, it is responsible for large-scale DDoS attacks to Dyn servers which is an Internet Service Provider (ISP). This attack was largely successful, as many people did not change the default logins of their devices. Numerous websites such as Twitter, Netflix, Spotify, and Reddit could not be available for a day [16].
- *Light Rail System Attack:* The light rail system of San Francisco in the USA was subjected to a ransomware attack. In the attack, no firewalls were breached but an employee invited the hackers into the system by clicking a phishing mail [17].
- *Water Company Hacking:* The attackers infiltrated water utility's SCADA system and they managed to manipulate the system to change the amount of chemicals used. Thus, they intervened in water treatment and production [18].
- *Smart Building Attack:* Smart homes and buildings are the general applications of IoT. The applications are developed via IoT devices and stay connected to the Internet continuously. The DDoS attack shut down heat and hot water systems at two buildings in winter. The DoS attack flooded the building control system with bogus Internet traffic. So, this caused to restart the system every few minutes and denying administrators remote access to the device [19].
- *Electric Grid Cyber-attack:* On the day of general election in UK, an electricity supply network was attacked. The aim of the cyber-attack was to infiltrate into the SCADA system to fail the electricity grid. The attack was carried out using some fake e-mails targeting senior employees. The e-mails included social engineering techniques to click on a fake link to trigger malware. This attack was a spear phishing attack which is the smarter version of phishing [20].
- *Petrochemical Plant Cyber-attack:* A failed cyber-attack against a petrochemical plant was carried out. The aim of the cyber-attack was to sabotage the operations of the facility and to cause an explosion that could kill people. Fortunately, an error in the source code of the attackers did not enable that the explosion occur. In other words, the only reason it was not happened, there was a mistake in the attackers' source code. Also, the source code was not seen in an earlier cyber-attack. All of the IoT-based hacking tools were custom-built [21].
- *Transport Network Cyber-attack:* The cyber-attack hit the transportation network causing train delays and disrupted travel services. Customers were unable to make reservations or receive updates about the delays [22].
- *Healthcare Company Cyber-attack:* A sophisticated attack was carried out to a healthcare company. Firstly, the attackers seized login information from a vendor who provides IT devices to the hospital. Secondly, they targeted a server by using remote execution techniques for SamSam ransomware. Finally, they encrypted the hospital's critical data files [23].
- *Telecommunication and Finance Sectors Cyber-attack:* An organized attack was carried out against the prominent institutions which provide communication infrastructure and financial services. The attack was aimed denial of services on critical infrastructures. The institutions that were attacked could not serve for a time[24].

TABLE 1
Some of IoT-based cyber-attacks on critical infrastructures between 2008 and 2019

Ref.	Year	Attack name	Attack location	Target of attack	Definition of attack	Damage of attack
[10]	2008	Tram hacking	Lodz city/Poland	Hacking the tram system by tripping rail switches and redirecting trains	Cyber-kinetic attack	Four trams derailed, some passengers were injured
[11]	2009	Power company hacking	Texas Power Company	To cripple power forecasting systems	Login into the VPN	Crippled the firm's energy forecast system for a day
[12]	2010	Stuxnet	Iranian nuclear facility	SCADA systems by targeting PLCs	Malicious computer worm, replay attack	Damaging of uranium enrichment centrifuges
[13]	2011	Water distribution system hacking	South Houston/Texas	To show how easy hacking the water distribution system	Password attack, remote attack	Usernames and passwords were stolen, The SCADA was powered on/off, burning out a water pump
[14]	2013	Dam cyber-attack	Bowman Avenue/NewYork	To gain unauthorized access to the SCADA system	Google dorking, advanced malicious tactics and techniques	The attackers gained control of the floodgates, but no physical harm was reported
[15]	2015	Power grid hacking	Ukraine	To sabotage the critical infrastructure	The BlackEnergy3 malware, Industroyer, and Crash Override	A massive power outage, approximately 225,000 customers without power for several hours
[16]	2016	Dyn (An ISP) attack	USA	To make web traffic of Dyn unavailable with Mirai botnet	DDoS attack	Access to popular websites disrupted and massive portions of the Internet shut down
[17]	2016	Light rail system attack	San Francisco/USA	Forcing the agency to temporarily run its service for free in ticketing booths	Ransomware attack, phishing	N/A
[18]	2016	Water company hacking	USA	To manipulate the valves controlling the flow of chemicals	SQL injection and phishing	Stolen accounts of costumers, changing the amount of chemicals used
[19]	2016	Smart building attack	Lappeenranta /Finland	Jamming the smart home management system with bogus Internet traffic	DDoS attack	Shut down heat and hot water in two buildings
[20]	2017	Electric grid cyber-attack	United Kingdom	To infiltrate the SCADA system for an electricity blackout	Spear phishing attack	N/A
[21]	2017	Petrochemical plant cyber-attack	Saudi Arabia	To sabotage the operations of the facility and to cause an explosion	A new kind of cyber-attack (much more dangerous than Shamoon attack)	An unsuccessful cyber-attack
[22]	2017	Transport network cyber-attack	Sweden	To crash the IT network system	DDoS attack	Taking down email systems, websites, and road traffic maps
[23]	2018	Healthcare cyber-attack	Indiana/USA	To obtain money from the company using ransomware techniques	SamSam ransome malware	The company paid 55,000 dollars ransom to hackers to regain access to its computer systems
[24]	2019	Telecommunication-Finance sectors cyber-attack	Turkey	To crash the communication networks of some national infrastructure sectors	Organized DDoS attack	Communication loss in the infrastructures temporary

Critical infrastructures enable more efficient performance and communication through IoT-based applications. But this can lead to security vulnerabilities and increase the number of cyber-attacks against critical infrastructures. In this study, the prominent IoT-based cyber-attacks are highlighted. In order to understand the severity of the situation, it is important to evaluate the effect and consequences of the mentioned cases. In this context, the whole cases emphasize the vulnerabilities in critical infrastructure systems. These vulnerabilities often depend on insecure setups in the IoT-based control systems. The aforementioned cyber-attacks are presented in Table 1 according to the year, location, target, definition and damage. Reference [25] may be examined for more cyber-attacks against critical infrastructures.

2.2. Common types of cyber-attacks

A cyber-kinetic attack targets IoT-based applications and Industrial Control Systems (ICS). This type of attack threatens human life, physical well-being or the environment. Cyber-kinetic attacks on IoT-based critical infrastructures are often complex. They are performed using multiple different methods and techniques. The most common methods used in these cyber-attacks are presented in this sesection.

- *Malware injection* is the settlement of malicious software into cyber-space to cause damage or to disable the system [26]. Adware, keyloggers, worms, spyware, rootkits, ransomware, trojans or viruses are prominent malware. WannaCry ransomware is a famous malware example. It is used to deny people's access to their files and essential services unless a ransom is paid.
- *Phishing* is a data request attack from an untrusted source. The untrusted resource tries to convince users that it is a trusted source. If the victim is convinced that the attacker is a trusted source, he performs certain actions that the attacker has identified before, such as clicking the malicious link and entering sensitive data. In this case, the victim gives his sensitive data to the attacker with own hand. If the victim is an employee in a critical infrastructure system, the situation can turn into a disaster.
- *Spear phishing* is the most common phishing attack, especially in critical infrastructures. Email attachments are used to make the user click on a link to trigger malicious software [27]. Although spear phishing is considered as one of the least complex methods of cyber-attacks, it has recently led to catastrophic effects on critical infrastructures. Therefore, the low level of cyber-security awareness is potentially the highest risk of cyber-attack in IoT-based critical infrastructures.
- *Hacking* is the process of gain access to the system. The most important operation of this process is to obtain the password of the system. Hacking is usually done by using various methods such as brute force, man-in-the-middle (MITM), and social engineering [28].
- *Denial of Service* attacks aim to congest the infrastructure of a system network with excessive traffic and spam data. The system communication infrastructure is overloaded by too many unnecessary connection requests. This makes the system slow or inoperable [29]. DDoS attacks potentially can be performed on all devices connected the Internet, especially on backbone components.
- *SQL injection* attacks aim to steal, alter or delete database content. It is used to attack the data-driven systems. Attackers execute SQL query statements to access the database server of the system [30]. Almost all of the IoT-based critical infrastructures have databases.

- *MITM attack* aims to eavesdrop communication between the devices. Since the data transmission is transmitted through the attacker's device, the data transmission on the network can be sniffed and modified by the attacker. When data transmission has not a robust encryption algorithm, MITM attack can be achieved easily in IoT-based applications [31].
- *Advanced Persistent Threat (APT)* is a cyber-attack where attackers gain access to the network of a system and remain an undetected way in the system for a time. The aim of an APT is usually data theft. An APT requires a complex and advanced process and is generally supported by large organizations or nations [32]. Also, an APT process requires a high degree of stealthiness throughout a cyber-attack. Black Energy, Red October, Stuxnet, Dragonfly 2.0, and Duqu are some prominent examples of APT. An APT has several stages [27]. Initial Compromise, Establish Foothold, Escalate Privileges, Internal Reconnaissance, Lateral Movement, Maintain Presence, Complete Mission are the stages respectively.

Initial Compromise stage represents the techniques used by attackers to penetrate the target network by exploiting cyber-security vulnerabilities. Since IoT-based critical infrastructures such as smart grid are coupled with the Internet, network devices may be probed by attackers. Through social engineering techniques, especially with spear phishing, the attackers execute malicious code on the system.

Establish Foothold stage represents that after attackers seize an IoT network device, they try to control more devices in the system. Also, backdoors are used to establish an outbound constant connection from the system to the computers which belong to the attackers.

Escalate Privileges stage involves obtaining credentials that allow attackers to access more resources in the IoT-based system. Attackers try to gain access to administrator accounts. Password cracking and harvesting are prominent techniques used in this stage.

Internal Reconnaissance stage is the process of collecting data about the internal network, trust relationships, groups, users, files, and documents by collecting data about the compromised devices. Attackers may search for the data of last modified date, keyword, or file extension. Domain controllers, email servers, and file servers are the main internal reconnaissance targets.

Lateral movement stage includes actions related to infiltrating other IoT-devices, searching for sensitive data, credentials stealing, and reconnaissance. To do so, attackers must move laterally in the network and obtain higher privileges by using different tools. To move laterally in the network and remain persistent without being recognized, attackers collect data such as operating systems, services used in the servers, and network hierarchy.

Maintain Presence stage aims to continue the control of IoT devices remotely from outside the system network through the backdoors. Attackers can also hide their activities in the system by deleting the traces, logs of the compromised devices and encrypting the traffic.

Complete Mission stage means that the attacker achieves his aim. After the attackers obtain the relevant data from the IoT devices, they transfer the data using FTP, file transfer tools, or backdoors. Once the attack is completed, most attackers want to maintain access to the system.

As the number of mobile and IoT devices increase due to the opportunities presented by ISPs, cyber-security vulnerabilities in IoT-based systems will continue to rise. Therefore, IoT-based critical infrastructures will be tested by attackers according to their security limits. Also, personal and corporate data may be a goal of obtaining a ransom for cyber-criminals because of the increasing number of devices connected to the Internet.

3. Mitigating of cyber-attacks

New cyber-attacks emerge every day and it is very hard to eliminate all of them. However, the initial defense techniques have a big importance in terms of reducing the effects of existing and future attacks. Mitigating the effects of cyber-attacks includes both intrusion detection methods [33] and intrusion prevention methods [5], [34]. Some of the leading methods to mitigate the effects of cyber-attacks in IoT-based critical infrastructures are listed below.

Access Control: It is vital to determine which resources, data files, and components can be accessed by users and devices in advance. Also, the areas that the users or devices cannot access must be defined too [35]. Using predefined access rules reduces the possibility of malicious access to the network. Access controls such as Discretionary, Mandatory, and Role-Based Access Controls can improve cyber-security of the system against potential security threats. In remotely monitored and configured cyber-physical systems, such as IoT-based smart grid, access controls are very important to restrict the access of users and devices in the network.

Encryption: Attackers want to capture data from the system or IP packets. But providing encryption with strong encryption methods reduces this [35]. Therefore, when IoT applications are used in critical infrastructures, the traffic of IoT devices to and from the control system must be effectively encrypted. However, using lightweight encryption techniques in IoT applications may create cyber-security problems. So, encryption is very crucial to protect data integrity and confidentiality in communication networks.

Authentication: Device authentication is the primary step in the secure data transmission session. It is responsible for identifying devices and authorizing the tasks that devices must do in the network. Time-sensitive is very crucial for IoT-based CPS communications. Therefore, an authentication scheme must include the least exchange of messages between the components. Authentication ensures that smart devices do not accept unauthorized commands [35]. Authorization and identification are included by authentication.

Regular and remotely security updates: IoT devices need to be easily updated in a manageable way. So, security updates of devices can be done simply too. If an IoT device is not configured to receive the updates, ensuring security updates may be a hardship. Unfortunately, most developers are currently developing IoT devices without considering firmware and security updates. However, due to the fast improvements in technology, it is important to provide updates effectively to address issues that operating systems and source codes may face due to security vulnerabilities [10]. Also, for an IoT-based smart grid, regular updates of the firmware is a logical solution as compared to large-scale replacement of the out-of-date devices. Moreover, updating of firmware remotely and easily is an important security requirement to mitigate potential threats in IoT-based systems.

Physical security: It is very important to ensure the physical security of the devices in the system. Tamper-proof mechanisms must be integrated into the system components to protect them against physical unauthorized access [36]. Accessing devices physically by unauthorized people may compromise the stored data in the devices. The stored data may be about identification, account, and authentication. Therefore, devices should have capabilities such as deleting or locking the data against physical attacks to protect if intruders capture the device. Moreover, it should be remembered that the physical security of the control rooms and the servers are more important. As a result, the physical security vulnerability of any device poses a risk for the entire network. So, precautions should be taken at the infrastructure installation stage.

Backdoors and login process: IoT solutions for critical infrastructures should ensure the data privacy and confidentiality of end-users. Therefore, manufacturers should assure that backdoor and malicious codes are not embedded in the devices during production. There are discussions about adding a backdoor using for legal surveillance on some IoT devices [10]. However, It is important to note that this back door is the same one used by attackers who attempt to gain illegal access to devices. Also, in mass-produce devices, unique logins should be created for each device, instead of the common default login password. Therefore, it would be hard for intruders to compromise devices and to participate them in a botnet for DDoS attacks.

IP fast hopping: DoS attacks are the most damaging attack type for IoT systems. So, a network layer software security solution can be an efficient way to mitigate DoS attacks. IP fast hopping provides an easy way for clients to hide content and destination server of their communication sessions [37]. An IP address pool which includes some router IP addresses from different networks is used to hide the real IP address of the destination server. This technique prevents identifying data transmission destination by attackers. Changing the server IP address is done in real-time on both the authorized clients and the server according to a unique schedule.

Intrusion Detection Systems: The aforementioned cyber-attack mitigation techniques are effective to defend an IoT-based system generally against external attacks. However, if the attacker is already in the system, the mentioned mitigation techniques may be inadequate. Therefore, intrusion detection systems are crucial to identify and counteract to compromised devices or networks [38]. Also, an IDS can help to use early warning systems taking appropriate countermeasures to mitigate future attacks. Four techniques used in IDSs are as follows:

1. Signature-based IDS compares the potential threat with the previously recorded attack type in the database. Attacks' signatures are stored in IDS database. Signature is a set of rules used to detect already identified attacks in IDS database and precaution with determined actions. If a new type of threat which is not stored previously in IDS database occurs, it can be a big vulnerability for the system. This is the limitation of signature-based IDS.

2. Anomaly-based IDS is designed to detect unknown attacks. Creating a reliable learning model using machine learning methods and then comparing new behaviors with this model is the main target of anomaly-based IDS. Although this approach allows the detection of previously unknown attacks, it can generate false alarms.

3. Host-based IDS is installed on a host and has a limited view of the whole network topology. Therefore, It can only detect malicious activities for the host where it is installed. It is often used to monitor any attack attempts on critical servers. Moreover, once the system is compromised, it can be disabled by attackers and this is a vulnerability for the system.

4. Stack-based IDS is the latest IDS technology. In this method, IP packets are monitored before they reach the upper layers according to the OSI layer model, in other words, before the packets are processed by any application or operating system.

The security of IoT-based environments such as critical infrastructures is a critical issue. IoT networks are one of the main structures of critical infrastructures. Thus, any security vulnerability of IoT networks can directly influence the whole environment in which they are used. Designing a robust, lightweight, integrated, and high-performance hybrid IDS is an effective solution to detect different types of attacks in IoT-based critical infrastructures.

4. Conclusion

Countries have critical infrastructures such as electronic communication, energy, banking and finance, critical public services, transportation, and water management. Critical infrastructures subject to cyber-attacks for various reasons due to their importance. It is also clear that physical or cyber attacks never end. Therefore, every country has to take the most popular and safest current precautions for these infrastructures every time. Cyber-attacks on critical infrastructures may cause detrimental damage. Cyber-attacks against nuclear facilities, power grids, dams, and other crucial infrastructures are rising by the day. Also, even if a critical infrastructure system is aging, it must be defended against advanced cyber-threats. Moreover, the number of smart mobile devices increases day by day. Increased Internet connectivity of smart devices creates serious security vulnerabilities in IP-based networks. Therefore, cyber-attacks will potentially increase in the coming years. If very important and critical steps are not taken to solve security problems, it is obvious that damages resulting from cyber-attacks on critical infrastructures will lead to a nightmare for nations and organizations.

IoT applications are the most important structures in terms of enhancing performance and communication in critical infrastructures. However, all attacks that can be happened on the Internet can be performed in IoT environments too. Therefore, using IoT applications in critical infrastructures can lead to cyber-attacks that can be performed on the Internet.

In this article, we have introduced an overview of recent cyber-attacks against IoT-based critical infrastructures. Furthermore, we have presented common techniques and methods used in cyber-attacks performed on critical infrastructures. Moreover, we have discussed different contemporary cyber-security mitigation ways against these cyber-attacks. Especially using appropriate IDS techniques is an important cyber-security aspect as it helps taking countermeasures in advance, also it enables developing a predictive and proactive cyber-security posture for IoT-based critical infrastructures.

References

[1] M. Z. Gunduz and R. Das, "Internet of things (IoT): Evolution, components and applications fields," *Pamukkale University, Journal of Engineering Sciences*, vol. 24, no. 2, pp. 327–335, 2018.

[2] M. Abomhara and G. M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," *Journal of Cyber Security and Mobility*, vol. 4, pp. 65–88, Jan. 2015.

[3] U. D. Ani, J. D. M. Watson, J. R. C. Nurse, A. Cook, and C. Maple, "A Review of Critical Infrastructure Protection Approaches: Improving Security through Responsiveness to the Dynamic Modelling Landscape," *arXiv:1904.01551 [cs]*, Apr. 2019. arXiv: 1904.01551.

[4] A. Cardenas, "Cyber-Physical Systems Security," Jan. 2019.

[5] M. Baykara and R. Daş, "A survey on potential applications of honeypot technology in intrusion detection systems," *International Journal of Computer Networks And Applications*, vol. 2, no. 5, pp. 203–211, 2015.

[6] S. Sağıroğlu and B. Arslan, "Fighting with Cyber Terror and Terrorism: Threats and Precautions," in *4th International Conference on Computer Science and Engineering (UBMK)*, pp. 239–244, Sept. 2019.

[7] J. Pacheco, V. H. Benitez, and Z. Pan, "Security framework for IoT end nodes with neural networks," *International Journal of Machine Learning and Computing*, vol. 9, pp. 381–386, Aug. 2019.

[8] L. Horwitz, "Internet of Things-The future of IoT miniguide: The burgeoning IoT market continues," July 2019. Cisco.

[9] G. Tuna, R. Das, and V. C. Gungor, "Communications Technologies for Smart Grid Applications: A Review of Advances and Challenges," in *Smart Grid Analytics for Sustainability and Urbanization*, pp. 215–235, 2018.

[10] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 36–49, June 2019.

[11] L. J. Wells, J. A. Camelio, C. B. Williams, and J. White, "Cyber-physical security challenges in manufacturing systems," *Manufacturing Letters*, vol. 2, pp. 74–77, Apr. 2014.

[12] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security-A Survey," *IEEE Internet of Things Journal*, vol. 4, pp. 1802–1831, Dec. 2017.

[13] B. Miller and D. Rowe, "A survey SCADA of and critical infrastructure incidents," in *Proceedings of the 1st Annual conference on Research in information technology - RIIT '12*, (Calgary, Alberta, Canada), p. 51, ACM Press, 2012.

[14] C. Kim, "Cyber-resilient industrial control system with diversified architecture and bus monitoring," in *2016 World Congress on Industrial Control Systems Security (WCICSS)*, pp. 1–6, Dec. 2016.

[15] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, pp. 1–8, Apr. 2017. ISSN: 2474-9753.

[16] X. Liu, C. Qian, W. G. Hatcher, H. Xu, W. Liao, and W. Yu, "Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities," *IEEE Access*, vol. 7, pp. 79523–79544, 2019.

[17] N. Tariq, M. Asim, and F. A. Khan, "Securing SCADA-based Critical Infrastructures: Challenges and Open Issues," *Procedia Computer Science*, vol. 155, pp. 612–617, Jan. 2019.

[18] H. S. Sanchez, D. Rotondo, T. Escobet, V. Puig, and J. Quevedo, "Bibliographical review on cyber attacks from a control oriented perspective," *Annual Reviews in Control*, vol. 48, pp. 103–128, Jan. 2019.

[19] E. Luiijf, I. Žutautaitė, and B. M. Hämmerli, *Critical Information Infrastructures Security: 13th International Conference, CRITIS 2018, Kaunas, Lithuania, September,*. Jan. 2019.

[20] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services," *IEEE Communications Surveys Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.

[21] J. Wilkins, "Can biometrics secure manufacturing?," *Biometric Technology Today*, vol. 2019, pp. 9–11, Jan. 2019.

[22] G. Tonn, J. P. Kesan, L. Zhang, and J. Czajkowski, "Cyber risk and insurance for transportation infrastructure," *Transport Policy*, vol. 79, pp. 103–114, July 2019.

[23] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, July 2018.

[24] "Cyberattacks blamed for Sunday's internet disruption across Turkey," *DailySabah*, Oct. 2019.

[25] K. E. Hemsley and D. R. O. E. Fisher, "History of Industrial Control System Cyber Incidents," Tech. Rep. INL/CON-18-44411-Rev002, Idaho National Lab. (INL), Idaho Falls, ID (United States), Dec. 2018.

[26] Y. Mo, T. H. J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-Physical Security of a Smart Grid Infrastructure," *Proceedings of the IEEE*, vol. 100, pp. 195–209, Jan. 2012.

[27] M. Li, W. Huang, Y. Wang, W. Fan, and J. Li, "The study of APT attack stage model," in *2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)*, pp. 1–5, June 2016. ISSN: null.

[28] M. Z. Gündüz and R. Daş, "Social Engineering: Common Attacks And Countermeasures," in *9th International Conference on Information Security And Cryptology*, pp. 11–18, 2016.

[29] R. Daş, A. Karabade, and G. Tuna, "Common network attack types and defense mechanisms," in *2015 23nd Signal Processing and Communications Applications Conference (SIU)*, pp. 2658–2661, May 2015. ISSN: 2165-0608.

[30] D. Demirol, R. Daş, and M. Baykara, "SQL enjeksiyon saldırı uygulaması ve güvenlik önerileri," in *1st International Symposium on Digital Forensics and Security (ISDFS'13)*, (Elazığ), pp. 62–66, Fırat Üniversitesi, 2013.

[31] M. Z. Gunduz and R. Das, "Analysis of cyber-attacks on smart grid applications," in *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*, pp. 1–5, Sept. 2018.

[32] I. Ghafir and V. Prenosil, "Advanced Persistent Threat Attack Detection: An Overview," vol. 4, pp. 50–54, Dec. 2014.

[33] M. Baykara and R. Das, "A novel hybrid approach for detection of web-based attacks in intrusion detection systems," *International Journal of Computer Networks And Applications*, vol. 4, pp. 62–76, Apr. 2017.

[34] M. Baykara and R. Das, "A novel honeypot based security approach for real-time intrusion detection and prevention systems," *Journal of Information Security and Applications*, vol. 41, pp. 103–116, Aug. 2018.

[35] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. F. Wang, "Impact of cyber-security issues on Smart Grid," in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, pp. 1–7, Dec. 2011.

[36] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Communications Magazine*, vol. 51, pp. 42–49, Jan. 2013.

[37] V. Krylov and K. Kravtsov, “IP Fast Hopping Protocol Design,” in *Proceedings of the 10th Central and Eastern European Software Engineering Conference in Russia*, 2014.

[38] A. S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, and Z. Y. Dong, “Cyber security framework for Internet of Things-based Energy Internet,” *Future Generation Computer Systems*, vol. 93, pp. 849–859, Apr. 2019.