Analysis and Mitigation of Cyber-attacks Targeting Infrastructures Operated by IoT Systems

Raja Salih Mohammed Hasan[1], Nadia Mahmood Ali[2], Ihsan Jabbar Hasan[2]

2 Institute of Medical Technology-Al-Mansoor, Middle Technical University, Baghdad / Iraq

2 Institute of Technology, Middle Technical University, Baghdad / Iraq

Raja.Salih14@yahoo.com

تحليل الهجمات السيبرانية وطرق تقليل أثرها على منظومات انترنت الاشياء

م. رجاء صالح محمد حسن[1]، م.م. نادية محمود علي[2]، أ.م. احسان جبار حسن[2]

الجامعة التقنية الوسطى- معهد التقني الطبي المنصور, بغداد \ العراق
الجامعة التقنية الوسطى- معهد التكنولوجيا-قسم الاجهزة الطبية, بغداد \ العراق

ABSTRACT

Numerous countries have a high impact on providing the planet with critical infrastructures offering very important services employed in different fields such as water resources management, public services, power grids, telecoms, commercials and transportation. The increasing solutions in the IoT systems made it possible to exploit the internet connection services for supporting the critical infrastructures. The latest are being targeted by various types of cyber-attacks due to the advancement in internet services. Therefore, improving the security systems and the ways to detect the threats are highly required. Meanwhile, protecting the critical infrastructures from hostile cyber-attacks are of high significance. This article brings examination of a number of cyber-attack scenarios focused on critical infrastructures during the recent years, and highlights the most effective countermeasures for mitigating the most common types of attacks.

Keywords: IoT structures, Cyber-attacks, CMunter-cyber-attacks, mitigation techniques

المستخلص

في اغلب بلدان العالم ومن خلال مواكبة التطور المضطرد في التكنولوجيا استحدثت العديد من الخدمات في مجالات عدة مثل ادارة مصادر المياه، الخدمات العامة، شبكات الطاقة، نظم الاتصالات و المواصلات التجارية. الحلول التي قدمتها شبكة الانترنت قدمت دعما متواصلا للبنى التحتية لهذه الخدمات. مع هذا الانتشار جعل هذه الخدمات عرضة للهجمات السيبرانية بسبب التقدم الكبير في طرق الولوج لشبكة الانترنت مما جعل توفير انظمة تتولى كشف وتحليل هذه الهجمات فضلا عن تقليلها وتقليل اثرها امرا ضروريا. يقدم هذا البحث تحليلا لعدد من الهجمات السيبرانية التي تستهدف البنى التحتية للمنظومات العاملة بمبدأ انترنت الاشياء من خلال وصف لهذه الهجمات وطرق حدوثها فضلا عن السبل المقترحة للتقليل من اثرها.

الكلمات المفتاحية: منظومات انترنت الاشياء، الهجمات السيبرانية، الدفاعات المضادة للهجمات السيبرانية، طرق تقليل اثر الهجمات السيبرانية.

1 - INTRODUCTION

The internet of things has revolutionized the communication over networks of machines [Gunduz and Das,2018]. The designated system has made it easy to connect numerous devices and equipment over the internet. Furthermore, high amount of data is usually exchanged among these devices without any human interaction, and the number of these devices is getting higher by the hour. The new advancement of IoT systems is making it possible of the devices to be remotely processes and managed through the web [Abomhara and Køien,2015]. As much as the IoT systems seem promising, it brings many cyber security threats targeting vulnerable areas that are connected to vast networks resulting in potential gaps for the attackers especially in sensitive infrastructures. Therefore, some protective measures are needed for reducing such risks [Ani *et al*,2019].

There are vast Applications in IoT, which makes it possible for security regarded vulnerabilities to be targeted. The sensitive infrastructures usually have critical information and control capabilities which if fell under control of the wrong hands, it may cause tremendous amount of damage to these infrastructures [Cardenas,2019]. The Damage includes disconnecting the power from supplying a hospital, manipulate the cooling system of nuclear power stations, hacking a smart automobile that is still in motion for theft or destruction purposes, and even attacks targeting water supply systems causing shortage in water which is vital to people, animals, plants and industrial applications [Baykara and Das,2015]. Additionally, cyber-attacks targeting infrastructure on foreign soil is considered as an act of hostility and may lead to war [Sağıroğlu *et al*, 2019 and Pacheco,2019]. For that, countries now consider cyber security as one of the national security topics

due to the fact that the cyber treats can cause destruction of governmental buildings and firms in the physical world by hacking the control panels by rogue attackers, who they may even concentrate on the civic information and target government personnel.

This topic presents various scenarios of cyber-attacks that targeted different infrastructures occurred during the last fifteen years when it was earlier considered as classified intel and now it has been released to the public. The effect of these attacks reached sensitive systems that had such an impact on the government and national security as well as the economic and financial systems. Therefore, there were various solutions discussed in this paper in order to mitigate these threats.

This article discusses various common scenarios of cyber-attacks happened during the last decade focused on attacks targeting susceptible infrastructure. Additionally, there are some scenarios that focused on toxic effect of these attacks in addition to analyzing them. On the other hand, counter measures were also discussed in order to mitigate these offenses.

2 - CYBER-ATTACKS TO CRITICAL INFRASTRUCTURES

The threats have become quite capable of commencing cyber-attacks targeting the most known infrastructure technologies that have control on various vital networks. The latest consist of many subnetworks operating numerous services and they are growing over time, the more they grow the more vulnerabilities they bring along the way. One of the most popular offenses it attacking the control systems especially the one called SCADA that is capable of controlling the power grid infrastructures. It is a fact that the ones who code viruses and design them to target particular sections in the

country such as transport, finance, power stations, power plants, and water treatment systems are quite skilled. Countless devices operating based on Internet of Things are easy to integrate with many vital applications and control terminals and the number of these devices is very much rising to tens of billions and the estimate is rising by the hour and that makes the data integrity and security more and more challenging [Horwitz,2019]. Adding to that, the more the applications and employments grow the more threats they bring with them as different types of infrastructures will be exposed to cyber-attacks [Tuna, 2019].

2 - 1 Review of the Latest Attacks

One of the most promising solutions for improving the security of local infrastructure is by using systems that run based on the same Internet of Things Technologies, in other words it is crucial to use the internet for out daily applications and the designated security measures must connected to web as well with the aid of the advancement of internet employment and services. Since the fact that all the systems and infrastructures that needed to be protected are exposed to all kinds of threat. Hence, the latest may affect the functioning performance of IoT systems and applications due to the vulnerabilities the come with them that are at risk of being targeted by cyber-attacks. Therefore, their effects on the infrastructures were analyzed.

Hacking the tram-systems: There has been an incident occurred in the past when a young boy was able to hack his access through the metro control system with the aid of simple tools and changed the direction of train which was considered as of the earliest incidents that caused some damage to the train and some passengers were injured in the process [Kimani *et al*, 2019].

Hacking the power companies: One of the companies fired an employee and the latest took revenge by hacking their network and disconnecting the main systems from the power supply by using his authentication info which could not be banned in time by the administration control [Wells, 2014].

Nuclear facilities: There has been an incident that occurred the before commenced by America and the Israeli government on the Nuclear program of Iran aiming to destroy one of the nuclear facilities. The SCADA system was targeted in order to create an automated sabotage [Humayed, 2017].

Hacking the water supply: It's one of the popular attacks that focuses on the water and waste systems when one of the hostile organizations once targeted by uploading false schematics and wrong schedules in order to fail the development and maintenance processes. Although, the system security was setup using a tri password, the attackers had no struggle breaching their way in [Miller and Rowe, 2012].

Attacking the dam control system: The dam hacking brings one of the incidents that has happened by hacking access to a SCADA system controlling a dam, caused by attackers for manipulating the water levels as well as the temperature of the equipment used in the control center. The reports stated that the hostile attackers were able to gain access easily and made some changes to the water flow rate in addition to the amounts of chemicals used in water treatment. The attack also caused some destruction to the infrastructures of the affected area [Kim, 2016].

Attack on the power grid: One day, one of the popular companies in the field of electrical power generation in the United Kingdom, suffered from an attack that targeted the SCADA system in control of the supply

network and caused an outage in some areas. The network was attacked using spam letters that were focused on senior executives in the company. The spamming emails contained click baits and hidden links that directs to downloading harmful software [Stellios, 2018].

Attacking a chemical facility: An example of cyber-attacks targeting the chemical industry was when a group of hostile hackers attempted to hack their access and cause damage to the production line by creating and explosion able to harm the workers in the facility. Luckily, a glitch in the code was the reason for failing the attack. However, it could do more damage if it wasn't for the code error [Wilkins, 2019].

Targeting a transport control network: A cyber-attack once targeted one of the transport control terminals and manipulated the time schedule causing delays in the departure and arrival times. Numerous complaints were reported from customers about their struggles to make reservations [Tonn, 2018].

Hacking the healthcare section: One of the major companies in the field of healthcare suffered from an attack, the latest occurred in a hospital, concentrated on the server responsible for the logging credentials gained from an IT company who provided the medical equipment to the hospital. The technique used during the attack was called SamSam encryption software which was able to seize all the database of the hospital [Coventry and Branley, 2018] ,[Hemsley and Fisher, 2018] .

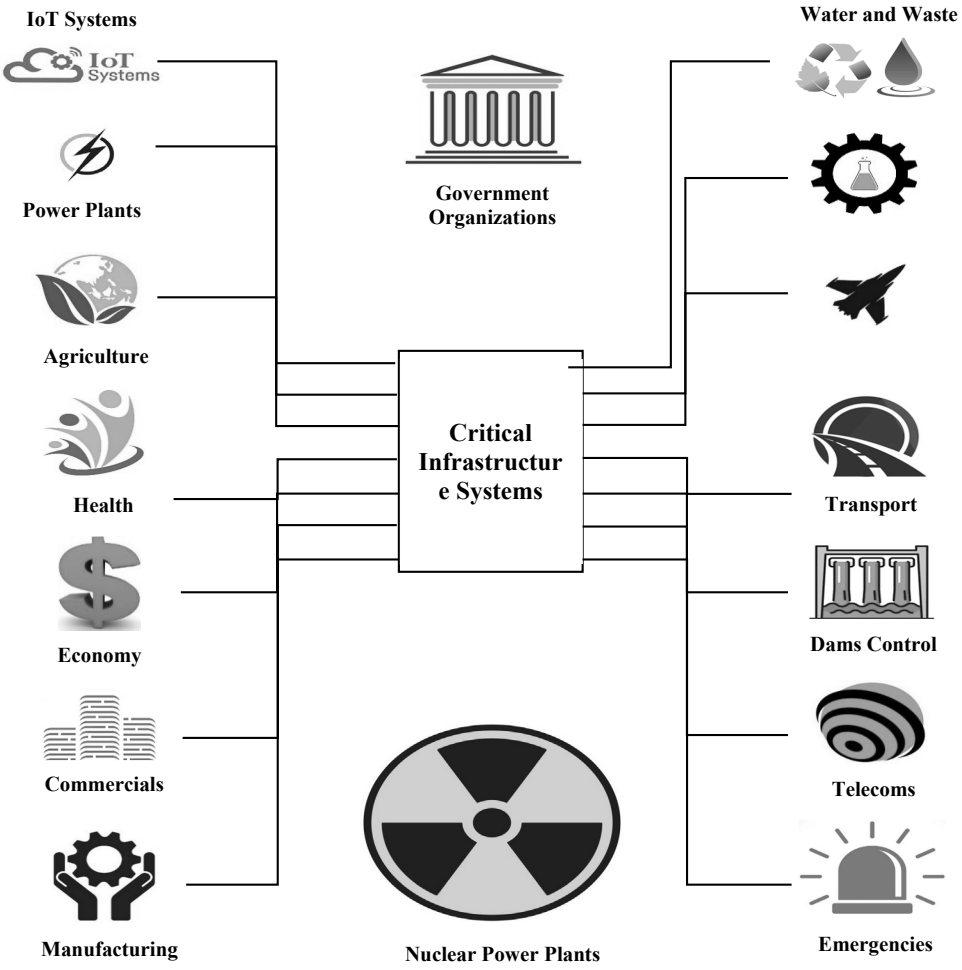

Fig. 1. tree of various infrastructure types

Ref	Date	Infra Type	Location	Target	Definition	Damage
10	2008	Tram System	Poland	Hacking the tram system terminal and changing the direction of tram vehicles	A cyber kinetic attack	Four of the tram vehicles were derailed from the rail way causing injuries to the passengers
11	2009	Power control systems	USA	Shutting down distribution power systems	VPN breaching	The attack was able to shut down the power distribution for the residential areas
12	2010	Stuxnet	Iran	PLC control systems of the SDADA control network	Malware worm attack	The attack caused damage to the uranium containers and centrifuges
13	2011	Water distribution system	USA	Illustration about showing the high possibility of hacking the water distribution system	Remote attack targeting the password database system	The attack targeted the SCADA system as well as the credential database causing the water pump to overheat

Ref	Date	Infra Type	Location	Target	Definition	Damage
14	2013	Cyber-attack targeting the Dam control system	USA	Gained unauthorized access to the SCADA system	Google dorking which is an advanced malware attack	The attack has caused the flooding gates to be opened but no physical harm was reported
15	2017	Power grid cyber attack	UK	The attack infiltrated the SCADA system of the electrical power grid	A spear phishing attack	No enough information available regarding the attack
16	2017	A petrochemical plant cyber attack	KSA	Sabotaging the operational facility causing an explosion	A recent attack type that is more effective than the attacks before	Despite the dangerous effect of the attack, it was unsuccessful
17	2017	A cyber-attack targeting the transport control system	Sweden	It was planned to target the information technology control system	DDos attack	Crashed the email systems and websites in addition to the road and traffic systems
18	2018	Healthcare system	USA	Ransom malware was used to breach the system and seizing it for money	Malware attack using the SamSam random type of malware	The attackers were able to receive more than 50K USD in exchange to retrieve access to the system

2 - 2 - Cyber Attack Types

There are numerous of applications that are operating based on IoT and they are targeted by kinetic cyber-attacks. The latest represent a direct threat to the individuals physically. Additionally, this type is complicated and they are carried out using various techniques. Therefore, this section will discuss the most popular cyber-attack types.

The Malicious injection: This method has the ability to disable the targeted system [Mo *et al*, 2012]. The popular ones are the Trojans mainly, then comes the ransomware, rootkits, spyware, worms, and keyloggers. And there is the WannaCry which is a ransomware, it's capable of totally seizing the data of users and prevents access to them unless the users obeys the rules of ransom.

The phishing attack: is one of the cyber-attack types that requires data requisition from one of the authorized access accounts. The attackers attempt to send a rogue link or fake invitation in order for the user to click on it and when the victim does, the link contains a virus to be automatically downloaded and perform a survey operation of all the login information stored in the victim's browser including bank accounts, company access information, social media accounts and other websites and portals.

The spear phishing attack :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 [Li, 2016]. 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 unauthorized entry into a computer, network or other systems with the intent to access data or to inflict damage. Hackers use their skills and knowledge to exploit vulnerabilities in systems, circumvent security measures or gain unauthorized access. There are various methods and techniques for commencing a hacking attack, it can brutally gain access through a particular system or by using the method of MTM which man in the middle or any other method related to social media engineering [Gündüz and Da¸s, 2016].

The denial of service attack: This kind of attack starts by flooding the targeted network by unwanted or unnecessary data traffic. The network equipment will be overwhelmed and the data contains so much dummy or rubbish data. As a result, the network will be very slow in responding to the data requests [Da¸s *et al*, 2015]. Any infrastructure connected to the web is compromised to this kind of attacks.

Attacks using SQL: injection which is one of the effective methods used in requisition, modification or disposing a database information. The method targets systems that usually operate based in existing data. The server that is designed to operate the systems is the one usually under the radar of attackers and they use SQL execution of query statements in the process [Demirol, 2013]. The reason that this method is quite effective due to the importance of database servers in almost all kinds of infrastructures.

Attacks using MITM: The main purpose of this kind of attacks is to spy on the communication between various devices infrastructure in any systems by making a rogue device in the middle between the peers. The process includes sniffing and editing by the hostile device. The attacks can be performed with any resistance if the transmission channels among the infrastructure devices were not protected properly [Gunduz and Das, 2018].

Cyberattack using Advanced Persist Threat (APT): This is one of the stealth attacks, though which the attacker gain access and remain undetected for a while. However, launching this kind of attacks is quite complicated and requires some advanced equipment that can only be owned by advanced and capable organizations [Ghafir and Prenosil, 2014]. Additionally, stealth is a must during this kind of attacks and it can only be maintained through sophisticated technologies. Many attacks have occurred using this approach such as Duqu, Red October, Dragonfly and others. The attack is known for having multiple stages [Baykara and Das, 2017], the first stage to begin with is the establishment of foothold, then comes the escalation of privileges, next there is the internal reconnaissance, followed by the lateral movement, and the next follower is maintaining the presence and finally comes the mission completion. These stages must be carried out in order.

The initial compromise: through this stage the attackers try to search for the vulnerabilities in the system in order to breach the network that is highly likely to be connected to the internet. The attackers must also keep track of all the devices connected to the targeted network. The social programmers mainly perform the necessary techniques such as spear phishing to inject and execute the malicious codes in the systems.

The footprint establishment procedure takes place after taking control of one of the network infrastructure and the attempt to take control of additional devices in the target system. Furthermore, the outbound continuous connection will be established between the system and hostile computer that is being used by the attacker.

The second stage includes escalating the privileges which involves breaching the credentials and gain access to all the assets and resources

in the system. Moreover, the hostiles try to hack their access to the admin accounts. Therefore, these procedures are essential during the first stage.

The internal reconnaissance stage represents the process of data collection of the system network information, trusted connections, workgroups, documents and users that can be collected from the breached devices. The hostiles during the attack could be searching data about the last edited date as well as keywords or they could be searching for the file extensions. The major targets during such attacks are the email systems, servers and domain controllers, in addition to the file servers.

The stage of lateral movements that involves infiltration of other types of IoT based devices, in pursuit of critical data such as authentication as well as reconnaissance data. In order to do such a thing, the hostiles attackers much be inside the network physically for gaining the high privileges aided by various tools and equipment. In order to move throughout the network, it's necessary to remain undetected and harvest data about servers, operating systems and other services and equipment in the network hierarchy.

The sixth stage is about maintaining the presence which is concerned with remotely controlling the IoT based devices that are stationed outside the network borders through the network backdoors. The hostile attackers usually don't leave any lead or trace behind, they even remove their activity from the log history.

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.

The final touch is the mission completion which, meaning that the hostile programmer accomplishes his tasks and they retrieve all the sensitive

data from the IoT based devices connected to the infrastructure using the FTP service along with the file transfer technologies and leave a backdoor for future access.

The growing advancement in the field of IoT causes a vast growth in the applications and devices. However, the more the technology advances the more risks appear in the systems especially when they are connected to the internet. Hence, the systems and infrastructures operating based on IoT should be tested by hackers in order to check for gaps and flaws that could be a target for the rogue hackers for seizing critical data and asking for ransom.

2 - COUNTERATTACKING THE THREATS

The security vulnerabilities are growing by the day and it bring difficulties to counter them all. The initial counter measures are a must to minimize the effect of future attacks. Countering the cyber-attacks should include detection for the possible threats [28] along with techniques for preventing the intrusion [Baykara and Da¸s, 2015] [Baykara and Das, 2018]. There are some effective methods that have been presented for mitigating several cyber-attacks and they are discussed below.

Built-in security systems: The production companies responsible for the networks and critical infrastructures equipment manufacturing should build security systems inside the systems. One of the most successful ways for improving the security of IoT systems is through understanding the fundamentals. All the companies responsible for the device production, the devices architecture, and the development teams as well as the systems designers must be on the same page through the design process to accomplish the maximum security possible and produce the most secured

equipment possible. The latest should be achieved by adding firewall techniques which will represent an additional line of defense using stronger encryption in addition to detection capabilities. When the companies fail to test their equipment, it will risk the confidence of clients and consumers. Therefore, it is necessary to include effective security systems to improve their reliability and hence the confidentiality of clients and consumers of IoT product whether they were private organizations or government agencies [Altulaihan, 2022].

Access Administration: It is necessary to categorize the access of data and system devices by which user based on relevant positions in the system in advance [Yang, 2011]. These access protocols are important for minimizing the possibility of a malicious attack to gain access to the network. The cyber security can be improved and by setting the access rules based on roles and positions and make the systems access more robust against potential cyber threats. These policies and protocols are necessary to monitor and configure systems operating over IoT including the smart power grids, dam controls, transportation and water supply controls.

In addition to the access control rules and policies, companies and organizations operating on IoT should increase the awareness and training of employees, engineers and IT staff about the threats and risks that they might face in their jobs, giving them an insight about the latest trends in security breaching techniques and educate them about the flaws and gaps in the systems that the hostile hackers might use to hack their access into critical infrastructures. Furthermore, they should be capable of making decisions in critical based on the information gathered from the devices [Polat, and Sodah, 2019].

Data Encryption: There is a limitation in the algorithms used in data encryption in IoT systems. Therefore, a plan to develop lightweight algorithms for cryptography purposes and create cipher codes to provide better data protection. In the meantime, different models of cryptographic techniques for generating lightweight cipher codes were proposed in [Polat, and Sodah, 2019] including SEA, KATAK/KTANTAN, mCrypton, LBlock and PRESENT. On the other hand, a number of researchers proposed implementation techniques for standardized cipher code blocks. Many application areas in IoT have a balance between its cost and performance as well as security. The levels of security in the electronic tickets are low. However, low levels of power and latency are needed. The parameters discussed in the paper mentioned the evaluation of more than fifty different code blocks of cipher cryptography which were classified based on various end nodes embedded with them. The paper also implied that there is a compromise in most of the lightweight and blocks of cipher codes which is due to their non-complexity, they might be vulnerable to Side Channel Analysis attacks. The latest are concentrated on IoT systems based on RSA, ECC and AES, the paper mentioned countermeasures for such hacking technique using Twofish which is a 128-bits code block of cipher cryptography. The research also highlighted some unique methods for generating cipher keys using physical Unclonable functions (PUFs) that is known for generating key codes for ID purposes. The technology does not involve embedding the cipher key in the IoT system, it derives it with the aid of PUFs from the ICs characteristics, this method is advantageous in terms of the low cost hardware [Iqbal, 2020]

Authentication control: One of the primary steps to maintain a secure transmission of data is through controlling the devices authentication

which is responsible for the identifications and authorization of devices through the network. The process of securing the network includes minimizing the transfer of unnecessary messages and files among devices [Bou-Harb *et al*, 2013]. Additionally, the files and information are monitored and authenticated throughout the network.

Remote security updates: The IoT based devices are needed to be continuously updated periodically and simply and they must be configured to make sure that they receive such updates. However, there are numerous production companies that do not send security updates to their client devices which make them vulnerable to future attacks. Therefore, there must be serious intentions to invest in the improvement technologies in order to reduce the effect of potential threats [Kimani *et al*, 2019]. The smart power grid is no less important application to be involved in the periodic security updates that can be provided remotely for countering the hostile activities.

Physical access: Locked racks should be used to secure the critical devices from getting physically accessed by unauthorized access along with terminating the wireless connections and using only wired connections instead. Additionally, all the unnecessary devices in the network should be disabled and lock the access ports by security protocols with high level of encryption while making the remote access to terminals and admin ports as limited as possible in order to prevent the attackers from discovering the critical devices and equipment are there in the network which will aid him knowing all the vulnerabilities and gaps for breaching in the network, enabling him to evade the red flags and detection mechanisms [El-Gendy and Azer,2020].

Log access and Backdoors: The IoT applications in sensitive infrastructures should protect that data integrity and privacy as well as the confidence of the end users for using the IoT based technologies. Hence, the production companies should stop embedding backdoors in their products that could be used as a gate for a lot of malicious activities by hostile attackers. In [Kimani *et al*, 2019], there's are many scenarios discussed about providing backdoors to the CCTV systems operating based on IoT. Additionally, there should be an alternative and unique way of accessing IoT devices operating for the first time instead of using the default authentication making it hard for rogue hackers to have access to these devices and compromise them to DDos attacks.

Fast hopping with IP: The attacks of Dos are considered as the most effective attacks in terms of damage done for the IoT devices and systems. Thus, the IP layer which is the network layer is an efficient method of countering this kind of attack. The IP fast hopping delivers a simple method of hiding both of the contents as well as the destination server from the point to point connection sessions [Krylov and Kravtsov, 2014]. The method hides the designated server IP address among a range of IP addresses provided by the router, which makes it difficult for the hostile hacker to identify the traffic and their destination. Additionally, the clients usually synch on the IP address change in real time.

The intrusion detection techniques: The cyber-attacks mentioned earlier were examples of effective ways of defending systems operating over IoT against various hostile attacks. On the other hand, there are some scenarios when the rogue hacker is inside the targeted network and that makes the countering techniques discussed earlier ineffective, and that brings on the

necessity of using the intrusion detection systems which have the ability to raise a flag when detecting a potential threat when compromising one of the major parts in any targeted network [Sani *et al*, 2019]. Furthermore, early warning technologies can initiate the countermeasures with the help of IDS for countering future attacks. The four techniques used are listed below:

1. The first type is the signature IDS that creates a comparison point between the current threat and the attack that occurred previously as recorded in a particular database. The signature of the hostile hacker is stored in that IDS database. The signature consists of multiple rules that have been set to identify previously recorded attacks in the database. However, if any attack type occurred to the system and it was not stored previously in the database, it can be a drawback to the whole system infrastructure.
2. There is another type of IDS based system which is the anomaly-based IDS, a system designed to detect any threat type that has not been stored previously in the database with the aid of machine learning, the method compares the behaviors of the anomaly based IDS with the previous attacks. The only flaw of this technique is that it could trigger some false alarms.
3. The host based IDS is a technique used to be installed on the host itself, but the host view of the network topology is limited, making it only able to trigger alert of malicious activities for a short a range in the network. This method is used for malware activity detection in the server areas only where the infrastructure is quite critical. The major downside of this technique is that it can be disabled once the network is breached by attackers.

4. Lastly, the stack-based IDS is a technique that monitors the IP packets in the OSI layers before get to the upper layers such as the session layer, the presentation layer all the way to the application layer.

The critical infrastructures in the IoT systems and environments are a sensitive issue and any part in the system network gets compromised, it will have an impact on the whole structure of the infrastructures. Therefore, creating a robust system with lightweight encryption algorithms and a significant performance is a must, IDS bring so much potential in maintaining the systems security by detecting all kinds of attacks and initial the proper countermeasures.

4. CONCLUSIONS

There are countless types of critical infrastructures all over the globe employed in numerous applications including, telecoms, power grids, commercials, public services, water supply management and transportation. These infrastructures are quite important to the national security and therefore they are at continuous risk of being compromised to many cyber hostile attacks. Every country around the globe is having security measures and precautions for protecting their critical infrastructures. The hostile cyber-attacks could cause much damage to these infrastructures, as they could be targeting power control systems, dams, and nuclear power stations and these risks always tend to rise. Moreover, the systems security is going out of date the technologies being used during the attacks are also being developed and improved, so should be the methods employed for mitigating the attacks.

The number of devices being employed in the IoT applications are increasing by the day inspired by the increasing performance of the internet services and the connectivity of small and embedded devices through numerous equipment and infrastructures. However, this inspiration brings high risks to the security of IoT which brings the necessity of improving the security systems and the security counter measure technologies in order to mitigate the cyber-attacks or reduce the impact of these attacks on the sensitive infrastructures.

Despite that the fact that IoT systems and applications are highly important when it comes to the performance levels as well as the communications quality especially when employed in critical infrastructures. On the other hand, the IoT systems are not untouchable, they make good targets to the cyber-attacks the moment they get connected to the web. This paper discusses an overview about the latest attacks on the IoT critical infrastructures. Additionally, various security breaching scenarios have been discussed with different technologies and methods used during the most common cyber-attacks in addition to the technologies used in the counter attacks. Different countermeasure techniques have been discussed including IDS as well as the predication and prevention methods for protecting the IoT infrastructures.

REFERENCES

- Abomhara, M., & Køien, G. M. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security and Mobility, 65-88.
- Ani, U. D., Watson, J. M., Nurse, J. R., Cook, A., & Maples, C. (2019). A Review of Critical Infrastructure Protection Approaches: Improving Security Through Responsiveness to the Dynamic Modelling Landscape.
- Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2022). Cybersecurity threats, countermeasures and mitigation techniques on the IoT: future research directions. Electronics, 11(20), 3330.
- Baykara, M., & Daş, R. (2015). A Srvey on Potential Applications of Honeypot Technology in Intrusion Detection Systems. International Journal of Computer Networks and Applications (IJCNA), 2(5), 203-211.
- Baykara, M., & Das, R. (2017). A Novel Hybrid Approach for Detection of Web-based Attacks in Intrusion Detection Systems. International Journal of Computer Networks and Applications, 4(2), 62-76.
- Baykara, M., & Das, R. (2018). A Novel Honeypot Based Security Approach for Real-time Intrusion Detection and Prevention Systems. Journal of Information Security and Applications, 41, 103-116.
- Bou-Harb, E., Fachkha, C., Pourzandi, M., Debbabi, M., & Assi, C. (2013). Communication Security for Smart Grid Distribution Networks. IEEE Communications Magazine, 51(1), 42-49.
- Cardenas, A. (2019). Cyber-physical Systems Security. The Cyber Security Body of Knowledge.
- Coventry, L., & Branley, D. (2018). Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward. Maturitas, 113, 48-52.
- Daş, R., Karabade, A., & Tuna, G. (2015, May). Common Network Attack Types and Defense Mechanisms. In 2015 23nd Signal Processing and Communications Applications Conference (siu) (pp. 2658-2661). IEEE.
- Demirol, D., Daş, R., & Baykara, M. (2013). SQL Enjeksiyon Saldırı Ugulaması ve Güvenlik önerileri. In 1st International Symposium on Digital Forensics and Security (1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu) (pp. 62-66).
- El-Gendy, S., & Azer, M. A. (2020, December). Security Framework for Internet of Things (IOT). In 2020 15th International Conference on Computer Engineering and Systems (ICCES) (pp. 1-6). IEEE.
- Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B., & Bangash, Y. A. (2020). An In-depth Analysis of IOT Security Requirements, Challenges, and Their Countermeasures via Software-defined Security. IEEE Internet of Things Journal, 7(10), 10250–10276. https://doi.org/10.1109/jiot.2020.2997651.

- Gunduz, M. Z., & Das, R. (2018, September). Analysis of Cyber-attacks on Smart Grid Applications. In 2018 International Conference on Artificial Intelligence and Data Processing (IDAP) (pp. 1-5). IEEE.
- Ghafir, I., & Prenosil, V. (2014). Advanced Persistent Threat Attack Detection: an Overview. Int. J. Adv. Comput. Netw. Secur., 4(4), 5054.
- Gunduz, M. Z., & Das, R. (2018). Internet of Things (IoT): Evolution, Components and Applications Fields.
- Horwitz, L. (2019). The Future of IOT Miniguide: The Burgeoning IOT Market Continues. CISCO, San Jose, CA, USA, Tech. Rep.
- Hemsley, K. E., & Fisher, E. (2018). History of Industrial Control System Cyber Incidents (No. INL/CON-18-44411-Rev002). Idaho National Lab.(INL), Idaho Falls, ID (United States).
- Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical Systems Security—A survey. IEEE Internet of Things Journal, 4(6), 1802-1831.
- Krylov, V., & Kravtsov, K. (2014, October). IP First Hopping Protocol Design. In Proceedings of the 10th Central and Eastern European Software Engineering Conference in Russia (pp. 1-5).
- Kimani, K., Oduol, V., & Langat, K. (2019). Cyber Security Challenges for IOT-based Smart Grid Networks. International journal of Critical Infrastructure Protection, 25, 36-49.
- Kim, C. (2016). Cyber-resilient Industrial Control System with Diversified Architecture and Bus Monitoring. In 2016 World Congress on Industrial Control Systems Security (WCICSS) (pp. 1-6). IEEE.
- Miller, B., & Rowe, D. (2012). A Survey SCADA of Critical Infrastructure Incidents. In Proceedings of the 1st Annual conference on Research in information technology (pp. 51-56).
- Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2011). Cyber–physical Security of a Smart Grid Infrastructure. Proceedings of the IEEE, 100(1), 195-209.
- M. Li, W. Huang, Y. Wang, W. Fan, and J. Li,(2016), "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.
- Pacheco, J., Benitez, V. H., & Pan, Z. (2019). Security Framework for IOT End Nodes with Neural Networks. International Journal of Machine Learning and Computing, 9(4), 381-386.
- Polat, G. and Sodah, F. (2019) Security issues in IOT: Challenges and Countermeasures, www.isaca.org. ISACA. The paper is Available at https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/security-issues-in-iot-challenges-and-countermeasures.
- Resul, D. A. S., & Gündüz, M. Z. (2020). Analysis of Cyber-attacks in IOT-based Critical Infrastructures. International Journal of Information Security Science, 8(4), 122-133.

- Sani, A. S., Yuan, D., Jin, J., Gao, L., Yu, S., & Dong, Z. Y. (2019). Cyber Security Framework for Internet of Things-based Energy Internet. Future Generation Computer Systems, 93, 849-859.
- Sağıroğlu, Ş., & Arslan, B. (2019). Fighting with Cyber Terror and Terrorism: Threats and Precautions. In 2019 4th International Conference on Computer Science and Engineering (UBMK) (pp. 239-244). IEEE.
- Tuna, G., Daş, R., & Gungor, V. C. (2018). Communications Technologies for Smart Grid Applications: A Review of Edvances and Challenges. Smart Grid Analytics for Sustainability and Urbanization, 215-235.
- Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). A Survey of IOT-enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services. IEEE Communications Surveys & Tutorials, 20(4), 3453-3495.
- Tonn, G., Kesan, J. P., Zhang, L., & Czajkowski, J. (2019). Cyber Risk and Insurance for Transportation Infrastructure. Transport policy, 79, 103-114.
- Wells, L. J., Camelio, J. A., Williams, C. B., & White, J. (2014). Cyber-physical Security Challenges in Manufacturing Systems. Manufacturing Letters, 2(2), 74-77.
- Wilkins, J. (2019). Can Biometrics Secure Manufacturing?. Biometric Technology Today, 2019(1), 9-11.
- Yang, Y., Littler, T., Sezer, S., McLaughlin, K., & Wang, H. F. (2011). 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). IEEE.