Critical Infrastructure Security in Healthcare Sector

A review of the Literature

IT19029214 | Hapuarachchi J.C
Sri Lanka Institute of Information Technology (SLIIT)

Mr. Kanishka Yapa
Applied Information Assurance | IE3022
10/05/2021

Critical Infrastructure Security in Healthcare sector: a literature review

IT19029214 | Hapuarachchi J.C

Faculty of Computing
Sri-Lanka Institute of Information Technology (SLIIT)

Applied Information Assurance

Abstract- Security in Critical Infrastructure in Healthcare Sector is challenging. This is challenging because, the infrastructure available in Healthcare Sector is very much critical and at the same time it is very much vulnerable. Cyber Crimes keep on increasing every day. Almost every sector in the world gets targeted by Cyber Crimes and out of these Health Sector takes a significant place. The review paper will highly focus on the current the challenges that health care sector face and why is healthcare sector crucial ad well as vulnerable. The main objective of this review paper is to summarize the current situation of Critical Infrastructure Security in Healthcare Sector. For this purpose, existing literature reviews that are written based on Critical Infrastructure Security in Healthcare Sector were reviewed. The information that was found are reviewed, analyzed, and presented in an understandable way. It is very important to make sure that the Healthcare Sector of any nation will get affected due to cyber-crimes. Although the required countermeasures and actions are taken to prevent the cyber-crimes in Healthcare Critical infrastructure, yet it is not 100% successful. The cybercrimes keep on increasing in a rapid scale. The review paper was done by doing a thorough research on the internet and by going through existing literature.

Index Terms- Critical Infrastructure security, Critical Infrastructure in Healthcare sector, Security Challenges for Healthcare Sector.

An Introduction to Critical Infrastructure Security in Healthcare sector

Cyber threats have been increasing during the past two decades. With the increasing technology cyber threats also increases parallel to that (John Soldatos, James Philpot and Gabriele Giunta,2019). Many of the organization, governments, companies, businesses or even individuals follow various methods to prevent from these kinds of cyber threats. But still, it is useless. No matter what method is followed it is impossible to prevent cyber threats 100%. But there is a capability of reducing cyber threats. Multinational companies and 1st world countries spends millions of dollars on cyber security, yet this is not 100% successful. According to the situation in a particular nation, the cyber attackers take advantage of it. During a war time, attackers targets at the military systems. Today, our world is a digitized world. Almost everything is digital. Digitized world enables the attackers to target a large portion of the world population (John Soldatos, James Philpot and Gabriele Giunta,2019). The attackers can even anonymously implement attacks and destroys the targeted system. Critical infrastructure is available in almost every sector in the world. Critical infrastructure can be systems, networks, network resources, assets (HealthCareCan,2017). Critical infrastructure is important for the continuous operation of a particular nation and economy. Cyber threats mostly target at the critical infrastructure of a particular sector. Critical infrastructure is available in almost every sector in a country like Healthcare sector, Defense and National security sector, Communication sector, Water sector, Transport sector, Educational Research and Innovation sector, Data and Cloud sector, Energy sector, Food and Grocery sector, Banking and Finance Sector, etc.

One of the sectors which is highly a target of cyber threats is Healthcare sector. If the attackers target the Healthcare sector, they can easily threaten the lives of millions of people. In health care sector almost, everything is digitized. As an example, the patient details are stored in computer databases, results of laboratory activities are stored in databases and even most of the patients connect with the databases using customized software applications. If by chance these databases get unavailable it will threaten the lives of hundred thousand of people. As an example, if a DDOS compromised, and this will make the databases unavailable to the hospital employees and will make the software application unavailable to the patients (John Soldatos, James Philpot, and Gabriele Giunta,2019). The damage cyber-attacks will cause is not money, but the lives of human beings. Cyber-attacks will easily

threaten the lives of patients. Because of this healthcare sector is very crucial. Not only cyber threats but also a particular sector should consider about physical threats as well. The Healthcare sector can either be public or private, no matter what it is, it has the possibility of becoming a target of an attacker. To protect healthcare sector from cyber-attacks, there are some few steps that healthcare sector should follow. First, the critical assets that can be targeted by cyberattacks should be identified, then need to find out what are the effects that will happen if these assets get compromised from an attack and then need to implement the counter measures to stop these kinds of attacks. It is also important to make the public aware about cyber-attacks. Most of the cyber-attacks happens due to the unawareness of public. Even the employees of Health sector should be aware about these kinds of attacks. The receptionist should be most aware about social engineering attacks, and the people who deals with computers should be aware about phishing attacks and other kind of viruses that can get infected to the computer, if they blindly download sources from unsecured websites available on the internet. If the employees of any sector are aware about cyber-attacks, then there is a possibility to decrease the happening of such kind of attacks to a certain extent and there are standards provided by various organization to follow such as GDPR (John Soldatos, James Philpot, and Gabriele Giunta,2019). If these standards are taken into consideration by organizations or nations it is possible to reduce cyber threats that will lead to cyber-attacks.

Research Statement/Objectives

Initially, the purpose of the literature review is to find out the existing literature and find out the challenges that are faced by Healthcare Sector when protecting critical infrastructure from cyber threats or cyber-attacks. While reviewing about these two, other aspects like interdependencies of Healthcare Sector, real world attack scenarios were found as well. To perform these, 15 different publicly available sources were used. Out of these 5 sources were thoroughly used because they were found more useful than other sources.

The main objective of doing a literature review on the existing literature of Critical Infrastructure Security in Healthcare Sector is to give the readers a clear understanding about the level of cyber security that healthcare sector possesses, the importance of Critical infrastructure in Healthcare sector, and why healthcare sector is vulnerable to cyber threats and cyber-attacks. Since this is a literature review this only pinpoint the important studies conducted by other respective people.

What is Critical Infrastructure?

According to a report on Critical Infrastructure in Canada's Health Sector presented by HealthCareCan (2017) critical infrastructure simply means the processes, systems or the assets that are needed to the survival, wellbeing of a particular sector or nation. This also helps to the well-being of the citizens and for the continuous functioning of operations in a nation. Almost Every sector has critical infrastructure. Critical infrastructure helps in the functioning and survival of a particular sector. As government of united states (October 1,2021) presents in critical infrastructure there are 16 critical infrastructure sectors. They are.

- Chemical Sector
- Communications Sector
- Dams Sector
- Emergency Services Sector
- Financial Services Sector
- Government Facilities Sector
- Information Technology Sector
- Transportation Systems Sector
- Commercial Facilities Sector
- Critical Manufacturing Sector
- Defense Industrial Base Sector
- Energy Sector
- Food and Agriculture Sector
- Healthcare Sector and Public Health Sector
- Nuclear Reactors, Materials and Waste Sector
- Water and Waste-water systems sector

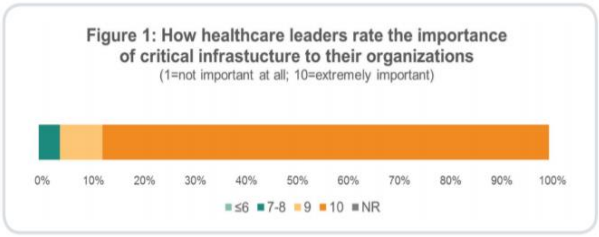
Since critical infrastructure is very important to the existence of various sectors, critical infrastructure have become a target of most of the cyber-threats. Recently several numbers of attacks have been happened that have targeted critical infrastructure of a particular sector. As an example, Henri Van Soest (2019) have stated about an attack that happened targeting a company name Elexon. This Elexon company is said to be playing an important role in United Kingdoms' electricity generation and moreover Henri Van Soest have also stated that although this attack was launched again Elexon however it was not successful. If by chance the attack got successful it will lead to unavailability of electricity in certain areas in United Kingdom. Another example of an attack which is reported in an Article presented by Allianz based on

Cyber Attacks on Critical Infrastructure is the attack launched by Iranian hackers to Bowman Avenue Dam and these hackers had the capability to gain access to the flood gates and according to Allianz, Energy Sector is one of the main sectors that are targeted by Cyber Hackers (Allianz, 2018). US cyber security officials available in Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) which is a government body of US who helps to investigate the attacks that launch against various networks and companies stated that cyber-attacks that happens against critical infrastructure and key manufacturing industries have increased during the last few years. US government body (ICS – CERT) also stated that there is an increase of cyber investigation by 15% in 2015 and there is an increase by double of the attacks happening against US critical manufacturing industries. Most of these attackers' goal is to target the control systems in a particular sector. Other than that, the attackers also target the data that these systems hold (Organizations of American States and Trend Micro, 2016). Even in the attack that happened against Bowman Avenue Dam, a data breach has occurred. Industries have become the target of most of the hackers, the reason for this is because these industries are responsible for various sectors in a nation. Edry stated that one of the most dangerous things today is the vulnerabilities which are available in technology and the lack of knowledge that public have about technology. He also stated that nowadays hackers are very much interested in launching attacks against operational technology and the devices that are physical connected in a specific network. Enry revealed about an attack happened against New York City Office block. In this scenario the attack had successfully gained access to the building management systems. The systems were said to be very crucial as these systems were controlling power, communication, and various other essential sectors. Enry stated the damage this attack caused. The attack resulted in an $350 million loss to the government (Allianz, 2018). Not only this, but there are also various attacks that have successfully launched targeting various industries and sectors. Cyber-attacks will not stop and it impossible to prevent these kinds of attacks 100%. Although government and private sector organizations take the necessary steps required to stop this kind of attacks, still some experienced hackers perform attacks and brings millions of losses to public and private sector organizations.

Critical Infrastructure in Healthcare Sector

According to the government of United States (October 1, 2021), Healthcare sector is one of the sectors that comes under 16 critical infrastructure sectors. This comes under the sector Healthcare Sector and Public Health Sector. Moreover, Cyber Security and Infrastructure Security Agency (CISA) presented Healthcare sector as a crucial sector. This is said to be because Healthcare Sector protects all other sectors from different kind of hazards such as infectious viruses, wounded people from terrorist attacks, wounded people from natural disasters and so many other kind of things and moreover CISA presented that for the continuous delivery of services of Healthcare Sector, it depends on some other sector like Communication Sector, Emergency Services Sector, Energy Sector, Food and Agriculture sector, Information Technology Sector, Transportation Systems Sector and Water and Waste Water systems Sector. For the continuous functioning of health sector, many of the sectors have an important role to play in this continuation process and in turn for the continuation of other sectors, Healthcare Sector plays an important role. These sectors are interdependent on each other. According to a report on Critical Infrastructure in Canada's Health Sector presented by HealthCareCan (2017), it is said that Healthcare Sector operates and uses the key elements of nation's critical infrastructure. Moreover, it presented most of the events that happens in a particular country affects Healthcare Sector.

When talking about critical infrastructure it is said that out of 10,9 health leaders have said that Critical Infrastructure is extremely important for their organization and simply these organization survives because of these critical Infrastructure. (HealthCareCan ,2017).



Source: HealthCareCan (2017)

From the ratings, it presents that critical infrastructure is essential to the continuation or survival of Healthcare Sector. It is a must to consider about the security of critical infrastructure and it is a must to take

the necessary steps and actions that are required to protect critical infrastructure in Healthcare Sector from cyber-attacks.

It is quite a challenge to protect critical infrastructure from cyber-attacks. Not only in Healthcare Sectors required controls or actions needed to take to protect critical infrastructure in any sort of a sector. This is a challenge because, the prevention of these kind of attacks is not easy and it is impossible to prevent them by 100%, but still there is a possibility to reduce the cyber-attacks thar are launched against critical infrastructure up to a certain extent.

Source: Thinkstock

Security Challenges for Critical Infrastructure in Healthcare Sector

Health sector is one of the most crucial and vulnerable sectors. Healthcare Sector helps to the continuation and survival of a particular country or nation. Critical infrastructure in Healthcare sector contributes significantly for this survival or continuation. It is important to protect the critical infrastructure in Healthcare Sector. It is challenging to protect these. Though it is challenging it is mandatory to protect these infrastructures. Cyber attackers will never stop doing unauthorized things. Most of the cyber attackers aims at the critical infrastructure of Healthcare Sector. If by chance critical infrastructure gets inaccessible it will cause a huge damage. The damage will happen financially, reputationally but most importantly it will threaten the lives of patients. As John Soldatos, James Philpot and Gabriele Giunta (March,2020) suggests in Cyber Physical Threat Intelligence For Critical Infrastructures Security, in Healthcare sector, there are Critical Infrastructure like;

- IT systems
- Hospital Information System (HIS)
- Picture Archiving and Communication System (PACS)
- Laboratory Information Systems (LIS)
- other vertical software like for ER-ED.

However, most of healthcare organization follows or have implemented various precautionary methods to reduce the cyber threats that are target on Critical Infrastructure Healthcare Sector. 1ST world countries such as America, England, Canada, Japan, and their allies have implemented the essential precautionary methods. Due to these implementations the happening of cyber-attacks remains very low (John Soldatos, James Philpot and Gabriele Giunta, March,2020). Moreover, they have mentioned that there is no possibility of happening of physical attacks to these critical infrastructures. The reason for this is because the servers and networks are not accessible for outsiders (John Soldatos, James Philpot and Gabriele Giunta, March,2020). Though they have mentioned like that, still there is possibility of physical attacks from insiders of a particular organization. Because some of the insiders have direct access to the server, networks, and other kinds of critical infrastructure. Another important fact the organization owners should keep in mind is that a particular hospital or a particular health care sector either it is private or public, they do not work properly without the IT systems, LIS and PACS. The reason for this is because the patients' related data are stored in these systems. As an example, a laboratory in a hospital cannot continue daily work without LIS. Not only that without PACS, it is difficult to work with radiological images. If these systems get effected or unavailable it will slow down the lab activities to a great extent (John Soldatos, James Philpot and Gabriele Giunta, March,2020). In Cyber-Physical Threat Intelligence For Critical Infrastructures Security it is stated in most of the hospitals in Europe protecting Healthcare Sector Infrastructure from Cyber-Threats is very much of a challenge, this is because of the lack of cyber security knowledge that these hospital owners possess and moreover they have mentioned that the IT systems of Healthcare Sector had to face number of malware attacks during the recent days and the damage which happened to some of the hospitals from these kind of attacks are more than expected. They have also stated that Ransomware attacks have had happened targeting critical infrastructure in healthcare sector.

Lastly it is important keep in mind, though it is challenge to secure critical infrastructure, still it is necessary and mandatory to take the necessary steps to prevent cyber-attacks and moreover though it is a known fact that cyber-attacks cannot be prevented by 100%, still if the necessary steps/countermeasures are taken, happening of attacks will remain very low.

Critical Infrastructure Interdependencies in Healthcare Sector

According to the report presented by American Society for Engineering Management (2012) that Healthcare sector depends on other sectors to perform its daily operations. Healthcare Sector cannot operate or exist without the help of other sectors. To perform healthcare operations, heath care sector uses components and systems that are owned by other different sectors. Davidson (2010) explained that Healthcare systems is a combination of other systems and components. Healthcare sector includes workforce, environment facilities, transportation data from other system components (that are not included in healthcare sector), etc. An example of this can be taken as the workforce which includes physician, Pharmacists, nurses, hospital attendants use transportations to deliver medicines and using ambulance services, etc. (Davidson, 2010). Moreover, since the technology keeps developing day by day, to a survival of a particular sector, other sectors also need to play a role (Thissen & Herder, 2003).

Moreover, it is important to keep in mind, to improve public healthcare sector, understanding the relationship between humans is important. Culture and global relationship should be understood to improve the services provided by healthcare sector (Sypek, Clugston, and Phillips, 2008)

Threats to Healthcare Sector

A cyber security threat or in other word cyber threat is an act which is malicious and will try to harm data, steal/corrupt data or damage the valuable system resources (Hugh Taylor, 2018). Threats tries to take advantage of the weaknesses that are available in systems.

Mainly there are 5 main threats that are faced by Healthcare Sector (Enisa, 2019)

- Malicious actions – These are the actions performed by unauthorized people or bad people with the intention of doing something malicious. Malicious actions can cause damage to the systems or system resources.
- Human errors – These errors can either be intentional or unintentional. No matter whether it is intentional or unintentional, it can lead to a damage to the systems. For example, human errors can lead to system vulnerability and attackers might take advantage of these vulnerabilities that are caused due to human errors.
- Natural disasters- Natural disasters are not preventable, but there is an ability to decrease the damage caused by natural disaster. Examples of Natural disasters are Fire, Flood, Earthquake, Landslides, etc.
- System Failures – In systems, failures can occur. These system failures are cyber threats. Attackers can launch attacks and make the targeted system fails.
- Supply chain failures- Suppliers comes under the category of third party. These third-party suppliers either intentionally or unintentionally might make mistakes.

A cyber threat/cyber attack can be carried out different kind of entities such as Threat actor (Internal or External), Malicious people, Remote attackers and also other things like things happen accidentally (John Soldatos, James Philpot and Gabriele Giunta,2019).

Real world attack Scenarios

Attack Scenarios taken from Cyber-physical Threat Intelligence for Critical Infrastructures Security, A guide to intergrate Cyber-physical protection of modern critical infrastructures by John Soldatos, James Philpot and Gabriele Giunta

Scenario 1: In 2017, a ransomware name Wannacry was launched against United Kingdom's National Health Service. This attack was successful and successfully infected around 300,000 computers from all around the world. This ransomware demanded the users of the infected computers to a pay ransom in bit coins. Wannacry attack successfully encrypted the data available in infected devices. This attack exploited a vulnerability which is available in windows. The attackers successfully infected 16 health sectors and from these 16 health sectors around 200,000 computers got infected. The attackers successfully did the bad thing which is where they cancelled around 20,000 appointments and paralyzed more than 1200 pieces of Diagnostic Equipment. However, the infected organization had to close their business for 10 continuous days and had to pay $17,000 ransom to the attackers.

Scenario 2: Another attack that happens often to Healthcare Sector is Medical Device Hijack which is also known Medjack. The goal of Medjack is to inject malicious malware to the medical devices that are not secured or vulnerable and if a particular medical device

gets infected, Medjack can move through the entire hospital network. It is stated that Medjack attack was first found to happen in 2015 and from 2015 up to now number of Medjack attacks have happened and detected. Medjack will infect the medical devices using various methods. As an example, Medjack will use social engineering, using USB devices that are infected, etc. This attack has different kind of variations which are designed to attack various medical devices that are available in a particular hospital. Medjack attack can attack devices like X-Ray machines and related X-Ray equipment, Picture Archive and Communications Systems (PACS) and various other systems and devices available in a hospital. If a particular device gets infected by Medjack, Medjack attack will install a backdoor to the infected device and will steal the unencrypted data that transmits through the hospital network.

Scenario 3: In 2019 on the month of January, a ransomware attack had launched against a Heart Specialist Clinic which is located Melbourne, Australia. In this attack, attackers successfully accessed the systems that holds the patients' data files. Because of the attack, patients' files were unable to access by the nurses and doctors and they were unable to access patients' detail file for 3 weeks continuously. Later it was identified that Heart Specialist Clinic have not followed the necessary cyber security countermeasures to prevent such kind of attacks and It is identified that even the basic countermeasure like backing up the required files are not performed.

Scenario 4: In 2018, an attack was launched against a Billing company in USA. This billing company operated online payments systems of 44 hospital networks. It was found that 2,652,537 of patients' record details are stolen. The data breach prevented the access of these details to the hospital networks.

Scenario 5: A phishing attack was happened targeting the New York health care sector. These attackers mainly targeted New York oncology and hematology clinic. The attack was successful because of the lack of knowledge the employees in the clinic had about phishing emails. 14 employees blindly clicked on the phishing emails. Using these phishing emails, attacker was able to get exposed to the health information which email accounts had.

Future Research

From the gathered literature reviews, there were gaps that were identified.

One of the gaps is that all the literature was done for the 1st world countries such as United Kingdom, Canada, Germany, and other allies. Cyber attacks that are launched against Critical Infrastructure in Healthcare Sector do not happen only in 1st world countries. It happens in 2nd world countries as well as third world countries like Sri Lanka. In future it will be much better if the researchers perform research on Cyber security threats that targets Critical Infrastructure in Healthcare sector in 2nd world countries as well as third world countries.

Another gap is that most of the research are done by targeting only one specific country. By conducting the research targeting only one specific country, it is difficult to get an idea about the overall Critical Infrastructure security in Healthcare sector in the world. In future research, it would be better, if the necessary people perform the research targeting various countries rather than targeting only one specific country.

In the research it would be better if the people who perform the research focuses on depth what are the drawbacks in Security in Critical Infrastructure in Healthcare Sector that leads to cyber attacks and what are the recommended countermeasures.

Conclusion

Healthcare sector have become more vulnerable to cyber attackers. The interdependency that Healthcare sector have with other sectors makes it more vulnerable to cyber-attacks. Because of interdependency, implementing security measures to Healthcare sector is challenging. If a system in Healthcare sector gets compromised it will cause huge damage in terms of finance, operations and will threaten the lives of Patients. Though it is not 100% possible to prevent cyber-attacks, still there is a possibility to reduce the happening of cyber attacks by implementing the required cyber security countermeasures. Another factor that makes Healthcare sector vulnerable to attacks is due to the lack of cyber security knowledge that workforce of Healthcare sector possess. No matter what controls are used, it is must to make the workforce of Healthcare sector aware about cyber-attacks Healthcare sector is not only vulnerable but also crucial. This cruciality is because healthcare sector deals with lives of patients. If a damage happens to healthcare sector it will inurn threatens the lives of patients; It is identified that one of the biggest challenges that healthcare sector faces is the protection of critical infrastructure from cyber attacks or cyber threats. Most of the time, the attackers compromise Healthcare

systems to perform a data breach and to block the operations of a particular hospital. Lastly it is important to state that, though it is challenging it is mandatory to implement the required countermeasures to protect critical infrastructure in healthcare sector from cyber-attacks.

Acknowledgement- I would like to express my gratitude to the lecturer in charge, Mr. Kanishka Yapa who guided us through the completion of this review paper.

References

[1] Luis Kun, "Protection of the Health Care and Public Health Critical Infrastructure and Key Assets", [Online]. Available: https://www.hawaii.edu/csati/summit/Protection_of_The_HC&PH_Kun.pdf [Accessed May. 13, 2021].

[2] CISA, "Healthcare and public health care sector", [Online]. Available: https://www.cisa.gov/healthcare-and-public-health-sector [Accessed May. 13, 2021].

[3] HealthCareCan, "Critical Infrastructure in Canada", [Online]. Available: https://www.healthcarecan.ca/wp-content/themes/camyno/assets/document/IssueBriefs/2017/EN/IssueBrief_CriticalInfrastructure_A.pdf [Accessed May. 13, 2021].

[4] National Health Information Sharing and Analysis Center, "Nation's Healthcare & Public Health Critical Infrastructure Leads Critical Infrastructure Cybersecurity Resilience", [Online]. Available: https://www.healthitoutcomes.com/doc/nation-s-healthcare-public-health-critical-infrastructure-leads-critical-0001 [Accessed May. 12, 2021].

[5] John Soldatos, James Philpet, Gabriele Giunta. (2020), "Cyber-physical threat intelligence for Critical Infrastructures Security: A Guide to integrated Cyber-Physical protection of Modern Critical Infrastructure" [Online]. Available: https://www.nowpublishers.com/article/BookDetails/9781680836868 [Accessed May. 11, 2021].

[6] Allianz, "Cyber-attacks on critical infrastructure", [Online]. Available: https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html [Accessed May. 13, 2021].

[7] Henri van Soezt. (2020), "Cyber criminals are now targeting critical electricity infrastructure", [Online]. Available: https://theconversation.com/au/topics/critical-infrastructure-15306[Accessed May. 13, 2021].

[8] CISA, "Critical Infrastructure sectors", [Online]. Available: https://www.cisa.gov/critical-infrastructure-sectors [Accessed May. 13, 2021].

[9] Alexis Quintal. (2021), "Preventing Cyberattacks and the Risk of Data Breaches to Critical Infrastructure ", [Online]. Available: https://www.prnewswire.com/news-releases/preventing-cyberattacks-and-the-risk-of-data-breaches-to-critical-infrastructure-301288224.html[Accessed May. 13, 2021].

[10] C Ariel Pinto. (2012), "Critical Infrastructure interdependency", [Online]. Available:https://www.researchgate.net/profile/Polinpapilinho_Katina/publication/279487920_On_critical_infrastructure_interdependency/links/57fabbeb08ae886b898622eb.pdf [Accessed May. 13, 2021].

[11] Elizabeth Snell. (2017), "Medical Device Cybersecurity Act Draws Industry Support ", [Online]. Available: https://healthitsecurity.com/news/medical-device-cybersecurity-act-draws-industry-support [Accessed May. 15, 2021].

[12] Deloittes, "Cyber Security for Critical Infrastructure", [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-public-sector-cybersecurity-critical-infrastructure.pdf [Accessed May. 15, 2021].

[13] Justin Snair. (2013) , “Risks of Cyber Attacks on the Healthcare Sector Leave Public Health of Communities Vulnerable”, [Online]. Available: https://www.naccho.org/blog/articles/risks-of-cyber-attacks-on-the-healthcare-sector-leave-public-health-of-communities-vulnerable [Accessed May. 15, 2021].

[14] Eva Maia et al. 2020. “Security Challenges for the Critical Infrastructures of the Healthcare Sector” in Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated CyberPhysical Protection of Modern Critical Infrastructures. Edited by John Soldatos, James Philpot and Gabriele Giunta. pp. 142–165. [Online]. Available: https://www.safecare-project.eu/wp-content/uploads/2020/09/8.-Security-Challenges-for-the-Critical-Infrastructures-of-the-Healthcare-Sector.pdf [Accessed May. 15, 2021].

[15] IEEE, “Cyber threats and counter measures in Healthcare Sector”, [Online]. Available: https://ieeeaccess.ieee.org/closed-special-sections/cyber-threats-countermeasures-healthcare-sector/[Accessed May. 15, 2021].

Author Profile

Name: Jayani Chamodhi Hapuarachchi (Hapuarachchi J.C)
Registration No: IT19029214
SLIIT E-mail: IT19029214@my.sliit.lk
Personal E-mail: jayanichamodhi11@gmail.com

I'm a young self-determined individual who loves to explore new things and learn new things in the world. I truly believe that "Miracle is just another name for Hard work". Moreover, I am a cyber security enthusiast who mainly focuses on Governance, Risk and Compliance (GRC) in Cyber Security.