REVIEW PAPER ON CRITICAL INFRASTRUCTURE SECURITY IN THE HEALTHCARE SECTOR

Sri Lanka Institute of Information Technology

IE3022-Applied Information Assurance | Assignment 01

Thissera P. T. D. | IT 19022666

Email: it19022666@my.sliit.lk

ABSTRACT

Healthcare organizations have a high potential to become an easy target for cybercrime due to their critical and vulnerable infrastructure. The rise of digitization has led to several security challenges. Identifying these critical challenges is a very important task not only from a technical point of view but also from a legal and managerial point of view.

It is also important to recognize the potential threats posed by the ability to fight cybercrime. This applies not only to physical or cyber threats, but also to combinations. Healthcare services have the potential to be influential and it is important to understand the ways in which they can be destabilized and how attackers use them to achieve their goals. It provides a brief overview of the critical challenges facing the healthcare industry and provides a list of recent safety events. Critical asset classification is also presented.

Index Terms – *Healthcare and Public Health (HPH), Artificial Intelligence (AL), Cybercrimes and Cyber Security, Internet of Things (IoT), RFID Technology, Security Information and Event Management (SIEM), Health Care Industry Cyber Security Task Force (HCIC)*

1. INTRODUCTION

Cyber security is one of the most critical components of the healthcare IT infrastructure. Cyber security risk-related risks are being introduced due to the rapid digitization of electronic healthcare reports and the provision of healthcare services from telehealth to mobile healthcare, such as "MHealth" and active medical devices over the network. These vulnerabilities are of particular concern as cyber-attacks can expose the most sensitive teeth and information in a healthcare environment or interfere with clinical care. Some cyber-attacks can severely affect the safety of patients. For example: betraying the integrity of data or disrupting the functionality of medical devices can harm a patient.

Medtronic embedded cardiovascular devices, ransomware attacks by programmers such as "NotPetya" and "WannaCry" are recent examples of weakening health care distribution capabilities. Healthcare organizations are particularly vulnerable to cyber-threats, and Verizon's data breach investigation report for 2018 revealed that data breaches are the most common in the healthcare sector. In addition, reports from several agencies show that nearly 80% of health care providers with health plans and health clearance homes, as well as those with electronic health records, have experienced data breaches in the past two years. Furthermore, studies have shown that at least two out of every ten health care workers write down their usernames and passwords, even though they are committed to demonstrating health care practices through programming.

There is a need to provide an overview of cyber security and healthcare, taking into account the importance of cybersecurity in providing safe, effective, and reliable healthcare. Systematic reviews in recent years have synthesized strategies from several articles on cyber threats to health care and from articles on how healthcare organizations have responded to cyber events. The study provided a comprehensive overview of health care systems, as well as understanding current trends, how to improve security through gap identification, and how various aspects of health care cyber security should be developed to guide future research efforts. Details of research conditions are also included.

2. RESEARCH STATEMENT/ OBJECTIVES

The core concept of this research is to study more than 15 sources in the field of healthcare and use that information to conduct research on current technologies in the field of healthcare, Critical Infrastructure Security in the Healthcare Sector, and future world healthcare development. It provides an in-depth study of topics such as ARTIFICIAL INTELLIGENCE (AI), CYBERSECURITY, CRITICAL INFRASTRUCTURE (CI), and the INTERNET OF THINGS (IoT) in healthcare sector currently attached to the healthcare sector around the world. It also focuses on the Health and Public

Health Specific Plan. The Health Care Industry Cyber Security Task Force (HCIC) released its findings to Congress on June 2, 2017, highlighting the urgency and complexity of the cyber security risks facing the health care industry, and the report focuses primarily on health care cyber security issues. There are issues with patient safety. It also states that everyone's support is needed in health care systems and in protecting patients from cyber threats.

Artificial intelligence (AI) is a technology designed to mimic human cognitive functions and bring about an ideal change in healthcare. This AI technology can also be applied to various types of health care data, structural or non-structured data. While this technology will be widely seen in the world of the future, it will enable us to make rapid progress in analytical techniques by increasing the availability of health care data. The report covers the facts of this technology from the study conducted.

The report also highlights some of the other new technologies that will help anyone with an interest in healthcare and the use of technology gain a proper understanding.

3. REVIEW OF THE LITERATURE

Health care structures include general precautions, functionalities, and cybersecurity solutions in these days. With these cyber security systems, the ability to successfully attack critical assets is at a very low level. For an examples: the main IT system, Hospital Information System (HIS), Image Preservation and Communication System (PACS), Laboratory Information Systems (LIS), and vertical software such as ER. [3] [4]

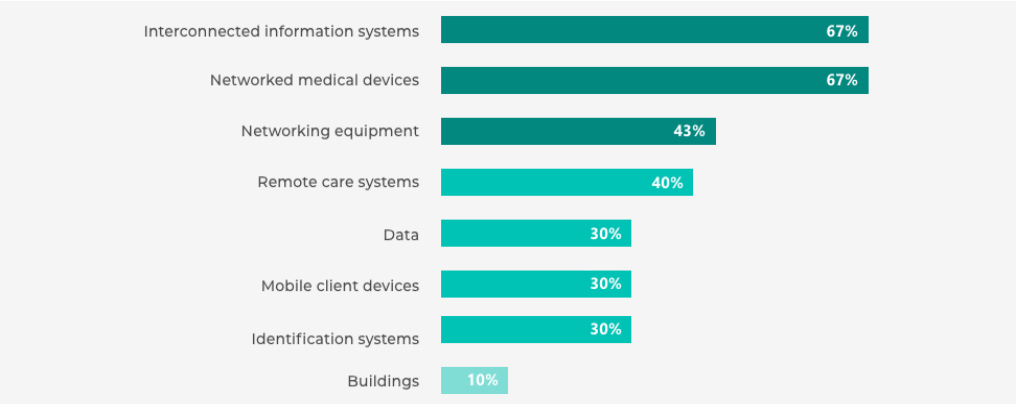

Figure 1

Because you need to connect directly to inaccessible servers and network sectors, you have no choice but to use a physical attack to protect the perimeter, and in this case, access with violence, theft, or other fraudulent access can be seen as a complementary function of a cyber-attack. Without an IT system, especially without PACS and LIS, health care structures will not function properly, and without it. It will be very difficult to deal with radioactive images and laboratory tests. It is also difficult to diagnose and for these reasons the diagnosis can be erroneous. Therefore, patients in health care facilities may develop a difficult or extremely slow treatment. This can be considered as offensive damage or "multiplication effect". For example, when the maximum number of casualties in a terrorist attack arrives at a hospital or health center, there is a risk that IT systems in hospitals or health centers will be attacked to reduce operational capacity or to absorb patients in the emergency department. Threats for that can no longer be analyzed as physical or cyber. It is important to develop a holistic approach to combating such a combination of threats.

According to the World Health Organization (WHO) definition, most parts of the health care system are productive and continue to provide services for acute and complex conditions. The health system has become an essential part of the day and supports the coordination and integration of care. It plays a key role in supporting other health care providers, such as primary health care, community services, and home care. For all of these reasons, cyber and physical attacks on health centers, patients, health workers, and health care facilities are on the rise around the world.

In terms of cyber-attacks, it is reported that about 80% of the surveyed healthcare organizations, and more than 100 million patients in the United States, compiled data to protect themselves from cyber-attacks in 2015. In addition, from 2009 to 2018, there were a large number of health care

data breaches, exposing nearly 189,945,850 reported thefts.

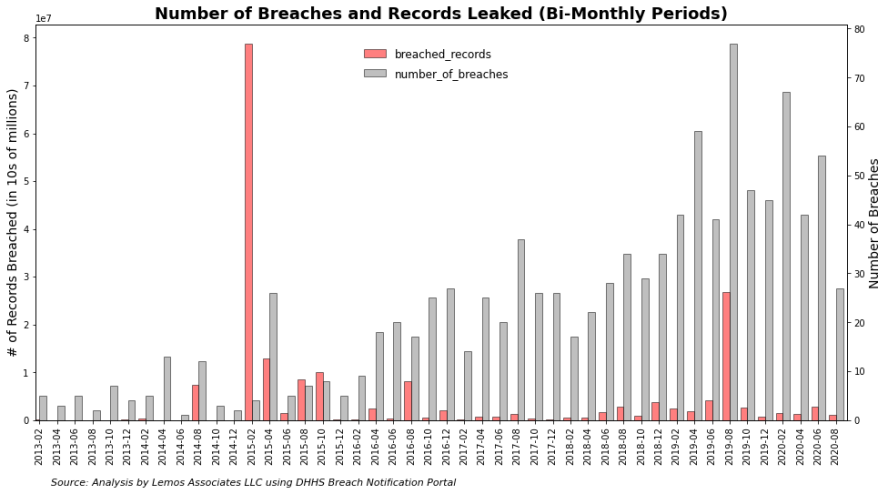

Figure 2

Figure 2: shows the number of beaches and records leaked in "Lemos" Associates LLC using DHHS breach notification porta from 2 months 2013 to 8 months 2020.

The leading attacks on health data breaches in the health sector are referred to as "unauthorized access" and "malware" including ransomware. Violations of these data and information can result in huge financial losses to healthcare organizations, as well as the reputation of the service provider and the deterioration of patient safety.

The Department of Health and Human Services in the United States has created a gateway to infringement. Its primary purpose is to gather information on recent physical security incidents in the healthcare sector, both physically and cyberbullying. According to that gateway, there will be attacks on about 400 institutions in year 2019 and a large number of individuals will be affected as a result. In addition, about 60% of major data and information infringements or IT incidents, nearly 1% of improper disposals, 25% of unauthorized access detections, and almost 5% of losses and theft are detected Has passed. It has also been able to detect unauthorized access and IT events affecting a large number of people. In addition, it has been revealed that health care providers have been involved in accidents and attempts to disrupt health systems.

The World Health Organization (WHO) created health care initiatives to systematically collect data and information on what constitutes an attack on health care, to advocate for an end to such attacks, and to promote best practices to protect health services from attack. Physical or cyber events greatly affect the provision of health care. It can also cause excessive stress, such as a lack of infrastructure or a large increase in patients. Not only can health care provide care, but it can also be seen as a last resort in the care of disaster victims. It also represents an icon of social security, relationships, and community beliefs. Thus, in this context, the resilience of a health service will be paramount, as will maintaining the levels of care provided and being able to raise and maintain service to the maximum level in any emergency.

3.1 INTERNET OF THINGS (IOT) IN HEALTHCARE SECTOR

IoT health applications are important for security due to the confidentiality of sensitive health data and information. Security solutions are classified to protect data from attacks.

Figure 3

Figure 3 : shows the data security of IoT healthcare applications.

Controlling access to IoT healthcare applications and the protection of health data and information can be considered a very important step. Care must be taken to enable IoT healthcare applications and devices through well-designed access controls. IoT devices collect health data and information from

patients and transfer it to health care databases. Therefore, it is of paramount importance that IoT healthcare applications also have very strong access management to ensure the security and privacy of that healthcare data. In addition to restricting the use of critical data to an organization, monitoring and privacy protection must also be performed, among the services to be provided by access control systems. In addition, it has become imperative for healthcare employers to be well-informed and trained in information security. In addition, employees should receive comprehensive training on priority access control to ensure data security, privacy, and patient rights.

Managing access to IoT healthcare applications can protect healthcare data and information from misuse and malicious attacks on users. Also, IoT health devices are very small, and it is another integrated system. These IoT health devices have also been able to collect various data from different environments. So having physical protection for these devices has become an important topic. Healthcare organizations have a role to play in protecting IoT health devices from physical threats, physical security of health data, environmental threats, accidents, physical disruptions, and theft.

It is advisable to have replacement equipment IoT Health Devices to protect against physical attacks. In this way, data collection and transfer activities are carried out continuously through these devices. These IoT health devices and applications are important for network security, while minimizing damage and retaliating for quick recovery from attacks, accidents, or disasters. All IoT devices connect to one or more networks and communicate with each other over that network or network. Therefore, network requirements are very important at every step of IoT health applications. Examples of some technologies are Wi-Fi, Bluetooth, RFID and ZigBee. Data is collected using devices that may be available, especially on a wireless local area network. Network security can be ensured by applying firewalls, applying IDS and IPS, applying login or advanced filtering structures, using secure socket layer or transport layer security (SSL / TSL), and using Internet Protocol Security. Messages should also be encrypted for applications using HTTPS.

3.1.1 RFID TECHNOLOGY

IoT health devices also connect to each other and exchange data using powerful encryption algorithms. That is, data is encrypted and then sent to the IoT application over a secure network. IoT devices use a technology called RFID to send data. This technology, called RFID, facilitates real-time monitoring and management of staff in all types of patient care environments in healthcare organizations. It provides useful data and information even when monitoring the productivity of a busy healthcare system. However, the Radio Frequency Identification (RFID) is said to have security vulnerabilities such as reverse engineering, man-made interception, and robbery. In addition, the IoT Health app must have robust access control management and trust management services to ensure both privacy and data security. The various health data collected through IoT health devices are shared by each unit, which uses that health care data to make an accurate assessment of a patient's diagnosis and make an accurate decision about treatment. There should be a principle to consider when delegating and managing the necessary requirements for a health care application. Furthermore, many health care standards are published by a number of international organizations. Those principles and documents are used to provide privacy and security. Every employee and every department in a healthcare organization should have significant data and information on guidelines, procedures, and standards related to data security and privacy. They can be modified to suit the needs of the healthcare sector by reviewing and updating them regularly. Training activities should be prepared to maintain and improve the health and data security of health workers. The training should provide information on basic safety and risks of IoT health care applications, as well as the privacy of data in healthcare services.

3.1.2 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Log monitoring, analysis and evaluation are done to prevent unwanted occurrences in a health care system. In addition, a central log management or Security Information and Event Management (SIEM) must be audited to ensure security. For that reason, all IoT healthcare devices, IoT healthcare applications, and all components of the network must be integrated with the ”Central Log Management System". Interruptions to unwanted incidents can minimize potential damage by alerting security teams quickly to those incidents. A Central Log Management System or Security Information and Event Management (SIEM) must have strong authentication and authorization to

better monitor the audit log. Also, the log should be checked continuously. An audit is a passive defense that raises awareness about critical security events after they occur so that they can respond quickly to unwanted events and help people.

3.2 ARTIFICIAL INTELLIGENT (AI)

In healthcare sector, artificial intelligence is a very broad term used to describe the use of machine learning algorithms and software or artificial intelligence (AI) to simulate human cognition in the presentation and understanding of complex medical and health care data analysis. In short, AI is the ability of computer algorithms to draw approximate conclusions based on input data.

AI technology differs completely from traditional healthcare technologies in its ability to collect data, process it, and deliver a well-defined output to the end user. AI does this through in-depth learning and the use of machine learning algorithms, which also have the ability to identify behavior patterns in algorithms and create their own logic. In order to gain useful understanding and prediction, machine learning models must be trained using extensive input data, and the AI algorithm behaves completely differently from humans. Algorithms can predict with great accuracy but will not provide an understanding of the logic behind its decisions other than the data and type used. [11], [14]

Figure 7

Figure 7: shows the AI technologies use in healthcare sector in the world.

The primary purpose of AI applications related to health care is to analyze the relationship between prevention or treatment modalities and patient-related outcomes. AI programs can be found in healthcare activities such as diagnostic procedures, treatment protocol development, drug development, personalized medicine decision making, patient monitoring, and care. The AI algorithm can be used to analyze large amounts of data from electronic health records for disease prevention and diagnosis. Departments such as the Memorial Sloan Kettering Cancer Center, medical institutions such as the Mayo Clinic, and the British National Health Service will develop AI algorithms to maximize their benefits. In addition, AI software is used in hospitals to enhance patient satisfaction and to initiate operations that meet the needs of their staff and workforce. The U.S. government has invested billions of dollars in the development of AI for health care. Healthcare companies are developing these technologies for healthcare managers to enhance business operations by increasing utility, reducing patient boarding, reducing stay time, and optimizing staff levels. Although the widespread use of AI for healthcare is a relatively new experience, the trend towards data privacy, job automation, and representation should be carefully considered before use. [15]

Example of AI technology used in the real-world health field: [17]

3.2.1 AI-ASSISTED ROBOTIC SURGERY

Analyzing data to guide surgeons by reducing 21% hospital stay. Such data can be used for future reference too which is minimal invasive. Results are always positive. A robot can also be used for both eye and heart surgeries. The accuracy and speed are greater than conventional methods.

3.2.2 VIRTUAL NURSING ASSISTANTS

Annual cost reduction by applying this is $ 20 billion. This can help to answer questions, monitoring patients in whole week and also can reduce hospital visits as well as can do wellness checks.

4. FUTURE RESEARCH

As health information technology products are widely available in healthcare delivery, health information technology will be a way to innovate. The research program should be carefully developed in the future, using scientific facts and technology to further strengthen the complex relationship between patient safety, their health information, and the technological applications of current health care. In recent times, critical infrastructure industries have been growing to a higher level. Through the interconnection of technology, can see the developments in Operational Technology (OT), Internet of Things

(IoT), Industrial Internet of Things (IIoT), cloud computing, big data, and other automated manufacturing. Many processes and products are transformed into digitization and in the future it will be possible to achieve greater productivity by making products using higher quality technologies.

Today, the healthcare sector is beginning to transform into a smart one. For example, the use of IoT BJC HealthCare, a healthcare provider, to transform the healthcare industry into a smart one, while providing meaningful real-time visibility through the supply chain while reducing costs and facilitating as well as increasing efficiency and operation. With the advancement of technology in critical infrastructure, the need and collection for physical and cyber security has increased, the ability to analyze large data, the digitization of health services, and the development of industries have also improved.

Advances in cybersecurity and physical security in industry, advances in cyber and physics, advances in robotics, advances on the Internet of Things (IoT), advances in industrial Internet activities, and advances in cloud computing will also be seen in the future. With the advancement of technology, there has been a huge growth in various fields such as telehealth in the healthcare context, the ability to provide better healthcare services using robotics, the development of wearable medical devices using IoT technology, and the advancement of mobile healthcare systems. The healthcare sector will be greatly affected in the near future.

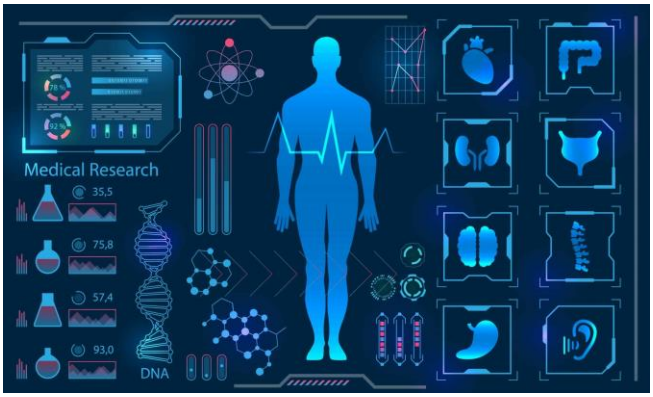

Figure 6

Figure 6: shows the technologies to be developed in the future world using IoT.

These studies explore one of the most important infrastructure components for healthcare, and whether critical infrastructure shifts will directly affect the future of healthcare. While conducting a research review on the exploration and development of this trend, critical planning is critical to the use of journal databases such as the IEEE and ScienceDirect in the review of the healthcare literature on the digitization of the healthcare sector and its future impact on healthcare.

4.1 INTERNET OF MEDICAL THINGS (IOMT)

IoMT is a small gadget that can connect with virus healthcare IT systems. Data that collected via IoMT can be shared with a physician through WIFI and it can also send them to closest people in order to get an idea of their health level. It monitors medical conditions specific to patient's disease and other systemic conditions such as heart rate, blood sugar, exercise , etc. [13]

Figure 7

Figure 7: The Internet of Medical Things is proving to be a godsend to the healthcare industry.

4.2 HYBRID CLOSED – LOOP INSULIN DELIVERY SYSTEM.

Also known as an artificial pancreas. This system specially innovated to manage type 1 diabetes. This system connects to a continuous glucose monitor with an insulin pump. It will help automatically manage such as situation with type 1 diabetes. People can mange their insulin level by their own.

4.3 VIRTUAL REALITY (VR)

VR is robust tool that give assistance to the health service bureau to execute exact diagnosis. This is combination of technologies which are used in MRI/CT scans. It will be a painless experience for patients. VR helps patients to be taken their surgical plans via virtual platform. [12]

Figure 8

Figure 8: Virtual Reality VR In Healthcare

4.4 MEDICAL TRICORDER

This is a movable scanning device easy to handle. This device has an ability to scan patients and get their virtual signs such as temperature and diagnose problems within a short period of time. It will help to save time & money and also it can be developed into such as specific categories. [20]

4.5 BIONIC CYBORG EYES

This is an experimental visual device which can use in surgeries instead of real eyes this item will help people who are with eye disease or totally blind and it accommodates, photodiodes and more light sense organ. Bionic Eye Technology is working with the Massachusetts Institute of Ophthalmology (MEEI) to develop a retinal diagram and obtain FDA certification. [19]

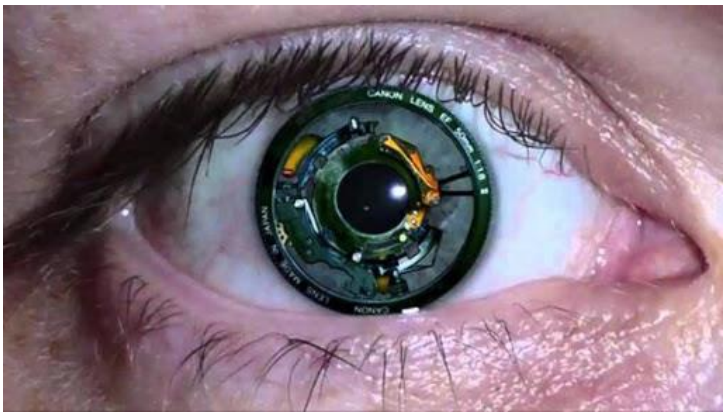

Figure 9

Figure 9: shows the bionic cyborg eye.

5. CONCLUSION

Healthcare organizations consider it a productive target for cybercrime. The increasing integration of cyber and physical systems and their eco-related devices poses a particular threat to these organizations and can bring new challenges from a challenging perspective. The cyber and physical controls of the health care sector must be systematically implemented to combat the threats posed by this age of health care technology. It should also minimize the potential harm to humans, property, and the environment.

In this chapter, the main security challenges of the healthcare environment are covered from a structural management perspective as well as a legal perspective. An inclusive survey of recent security events was conducted to understand the types of risks that are being exploited by attackers in the health sector. The threats and critical asset classifications posed by this research are also well defined. All this information will help you to have an understanding of the security issues facing the healthcare facilities in the smart hospital age.

6. APPENDIX

The news for critical infrastructure based on the Internet of Things (IoT) is encouraging, as IoT systems typically feature a large amount of data using sensors associated with clinical integration components. Empirical modeling can be used to capture, distribute, and manage CI data while acquiring sensors with the help of a context-aware data distribution service. Potential applications include smart cloud services that can integrate such data with other group-sources or group-sensors to support real and highly reliable analytics and intelligence. The networks, communications, and distribution that are typically required to solve the modeling process involve many complexities.

By combining sensitive data and historical data, it will be easier to observe and connect the interrelationships and interdependencies between critical infrastructure components, systems, and sectors. Thus, empirically based design techniques seem to best assist in identifying more repetitive, realistic, and suggestions. IoT is used to create these agent-based models to facilitate agents interacting with other agents so that the content contained in the critical infrastructure can be implemented without interruption.

7. ACKNOWLEDGEMENT

I would like to pay my respects to Sri Lanka Institute of Information Technology Applied Information Assurance (AIA) Model Lecturer Mr.

Kanishka Yapa. First, we were able to gain a better understanding of his concept through his articles on current and future practices in healthcare sector. He would also like to share his knowledge with us and honor us for guiding us in the right path. Also, it was great to be able to complete this research properly and to pay more attention to it by giving a detailed explanation in order to enhance our knowledge properly.

I would also like to extend my appreciation to my colleague Eradh Jayasundara, who has been instrumental in helping me in my research. Inspired by him, I was able to carry out this research better and see this research in new dimensions. I would also like to express my gratitude to all my family members for their innumerable methods and for saving me from many mistakes. I was able to enhance this study because of the generosity and uniqueness of everyone.

Finally, I would like to thank my university for furthering my education. I would like to pay my respects to creating thousands of people like me and paving the way for future conquests of Sri Lanka and the world. With my 100% commitment and full effort for any assignment given, I look forward to successfully completing and striving to conquer the world of tomorrow.

References

[1] P. F. M. M. William Hurst, "A Survey of Critical Infrastructure Security," IFIP Advances in Information and Communication Technology , March 2014. [Online]. Available: https://www.researchgate.net/publication/267391571_A_Survey_of_Critical_Infrastructure_Security. [Accessed May 2021].

[2] J. D. M. W. J. R. C. N. A. C. C. M. Uchenna D Ani1*, "A Review of Critical Infrastructure Protection Approaches: Improving Security through Responsiveness to the Dynamic Modelling Landscape," ResearchGate, April 2019. [Online]. Available: https://www.researchgate.net/publication/332169085_A_Review_of_Critical_Infrastructure_Protection_Approaches_Improving_Security_through_Responsiveness_to_the_Dynamic_Modelling_Landscape. [Accessed May 2021].

[3] "AI in healthcare," foresee, 12555 High Bluff Drive, Suite 100 , 2021. [Online]. Available: https://www.foreseemed.com/artificial-intelligence-in-healthcare.

[4] D. Marbury, "Six Healthcare Technologies Coming in the Next 10 Years," *MHE Publication, Managed Healthcare Executive,* vol. 29, no. 2, February 2, 2019.

[5] J. P. P. A VasquezMónica HuertaMónica HuertaRoger ClotetRoger Clotet, "Intelligent System for Identification of patients in Healthcare," *Security in Healthcare sector,* vol. 51, June 2015.

[6] B. Marr, "How Is AI Used In Healthcare - 5 Powerful Real-World Examples That Show The Latest Advances," Enterprise Tech, 27 July 2018. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2018/07/27/how-is-ai-used-in-healthcare-5-powerful-real-world-examples-that-show-the-latest-advances/?sh=7af0297c5dfb.

[7] M. J. Fritschle, "What Is the Internet of Medical Things and What Is Its Impact on Healthcare?," 11 Dec 2018.

[8] "Global Augmented Reality (AR) and Virtual Reality (VR) in Healthcare Market 2020: Trends, Industry Drivers, Opportunities, Challenges & Market Segment To 2026," Eon Market Research, 13 January 2021. [Online]. Available: https://www.medgadget.com/2021/01/global-augmented-reality-ar-and-virtual-reality-vr-in-healthcare-market-2020-trends-industry-drivers-opportunities-challenges-market-segment-to-2026.html.

[9] "Medical tricorder," Memory Alpha, [Online]. Available: https://memory-alpha.fandom.com/wiki/Medical_tricorder.

[10] Eugene Peretz/Flickr, "Artificial vision: what people with bionic eyes see," 17 Aug 2017. [Online]. Available: https://theconversation.com/artificial-vision-what-people-with-bionic-eyes-see-79758.

[I. P. V. M. I. G. By Eva Maia, "Security Challenges
1 for the Critical," NOW the essence of
1 knowladge, 2020. [Online]. Available:
] https://www.safecare-project.eu/wp-content/uploads/2020/09/8.-Security-Challenges-for-the-Critical-Infrastructures-of-the-Healthcare-Sector.pdf.

[G. Eysenbach, "Health Care and Cybersecurity:
1 Bibliometric Analysis of the Literature," Journal
2 of Medical Internet Research Publications, 15
] February 2019. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6396074/#idm139899973215760title. [Accessed 13 May 2021].

[H. E. Cansu Eken, "Security Threats and
1 Recommendation in IoT Healthcare," EUROSIM
3 2016 & SIMS 2016, Turkey, 2016.
]

[R. Lemos, "Dark Reading," 13 8 2020. [Online].
1 Available:
4 https://www.darkreading.com/attacks-
] breaches/healthcare-industry-sees-respite-from-attacks-in-first-half-of-2020/d/d-id/1338668.

[L. KUN, "Protection of the Health Care and
1 Public Health Critical Infrastructure and Key
5 Assets," February 2004. [Online]. Available:
] https://www.hawaii.edu/csati/summit/Protection_of_The_HC&PH_Kun.pdf. [Accessed 15 May 2021].

[G. J. C.-H. J. M. Y. Roberto Lacal Arantegui,
1 "Methodologies and applications for critical
6 infrastructure protection: State-of-the-art,"
] October 2011. [Online]. Available: https://www.researchgate.net/publication/227415351_Methodologies_and_applications_for_critical_infrastructure_protection_State-of-the-art. [Accessed 15 May 2021].

[A. &. E. A. Newsome, "Critical Infrastructure:
1 The future impact of," [Online]. Available:
7 https://www.ut.edu/uploadedFiles/Academics
] /Business/MIS/Ashley_Newsome_Ayush_Enkhtaivan_Research_Summary.pdf. [Accessed 15 May 2021].

["10 Ways Technology Is Changing Healthcare,"
1 The Medical Futurist, 3 March 2020. [Online].
8 Available: https://medicalfuturist.com/ten-
] ways-technology-changing-healthcare/#.

[M. J. Fritschle, "What Is the Internet of Medical
1 Things and What Is Its Impact on Healthcare?,"
9 2018 December 11.
]

[M. Bamiah, S. Brohi, S. Chuprat and J.-l. A.
2 Manan, "IEEE Xplore," 28 March 2013. [Online].
0 Available:
] https://ieeexplore.ieee.org/abstract/document/6488073.

["What is Healthcare and Public Health Sector
2 Critical Infrastructure Protection?," Pubic
1 health emergency, 8 Feb 2018. [Online].
] Available: https://www.phe.gov/Preparedness/planning/cip/Pages/about.aspx.

AUTHOR PROFILE

Thissera P. T. D

Born in Colombo, Sri Lanka on 23rd of July 1999. Studying at University of Sri Lanka Institute of Information Technology, Malabe, Sri Lanka. Received the certificate in INTRODUCTION TO CYBERSECURITY COURSE at Cisco Networking Academy, Sri Lanka, in 2020, INTRODUCTION TO IOT COURSE at Cisco Networking Academy in 2020 and NDG LINUX UNHATCHED COURSE at Cisco Networking Academy in year 2020. Following BSc (Hons) in Information Technology Specializing in Cyber Security degree, Sri Lanka Institute of Information Technology (SLIIT) University, Malabe, Sri Lanka, From February 2019 to February 2023. She worked as COMPUTER APPLICATION ASSISTANT at WebstazyOne software company,

Colombo 07. Her primary research interests include Critical infrastructure security in healthcare sector, Artificial intelligence, Internet of Things (IOT), Buffer overflowing attacks, security vulnerabilities, and Cyber Crimes and so on. Ms. Thissera is a member of IEEE community at SLIIT, Member of ISACA community in SLIIT and a member of Cyber Security Community in SLIIT. And she has number of achievements like ALL ISLAND, JUNIOR NATIONAL, INTER SCHOOL CHAMPIONSHIPS in BADMINTON. Ms. Thissera held number of positions in school level. Currently, she is in 3rd year 1st semester in her university life.