Critical Infrastructure Security in the Healthcare Sector

Eranda H.P.D
Cyber Security, Department of Information Systems Engineering
Faculty of Computing
Sri Lanka Institute of Information Technology
Sri Lanka
dilshan0627@gmail.com

***Abstract*—In all around the world, governments allocate billions & trillions of money annually specifically for the healthcare sector. The importance of that decision is clearly highlighted specially in a global pandemic situation like Covid-19. As a side effect of current trends in cyber warfare, cyber security has made a huge impact on our lives in all aspects. During the past several years, governments & organizations had overseen a rapid growth in cyber attacks. Specially, when it comes to the Healthcare sector, it is the one that is responsible for saving billions of lives of people & recovering from disasters while functioning 24 hours a day. So it's completely fair to allocate billions & trillions of money on healthcare sector. Currently in today's world, protection of this valuable healthcare system has become a very urgent task. But currently, this particular healthcare sector is under the influence of increasing amount of threats. As a result, protecting the healthcare sector from those threats & risks is a massive responsibility of all of us. The main objective of this review paper is to find out the potential threats & vulnerabilities in the healthcare sector and proposing countermeasures to prevent them.**

***Index Terms*—Public health, Critical Infrastructure, Data breaches, Threats, Risks, Sabotage, Privileges, Countermeasures**

I. Introduction

As we all know, currently the whole globe is facing a massive pandemic situation which is Covid-19. As a result of it, the entire healthcare sector has obviously become the most valuable & vital asset among all the other sectors. The main purpose of writing this review paper is to create awareness about different types of cyber attacks related to the critical infrastructure in healthcare sector. When conducting this research, Google Scholar and IEEE Xplore are used as existing literature reviews. Those literature sources include different types of attack vectors, types of threat actors, potential threats, risks & countermeasures. According to the current situation in the world, the existence of entire human race depends on this healthcare sector. At this stage, it has become very vital to defend this healthcare sector from potential threats and attacks. While currently the healthcare sector is responding to this pandemic situation, cybercriminals have locked their target on the healthcare system. Healthcare sector is not all about treating patients. It includes research & development, manufacturing, distribution, specialized tools & devices, administration of vaccines etc. Currently , all of those above mentioned sub-sectors have been exposed to cybercriminal attacks. A critical infrastructure is all about a group of assets. When the healthcare critical infrastructure is considered, it depends on electrical supply critical infrastructure, transport critical infrastructure, water supply critical infrastructure and communication critical infrastructure etc.

When it comes to the cyber attacks, usually there are two types of attacks, which are inside attacks and outside attacks. Among those **"Inside Attacks"** has become more aggressive & more frequent when compared to the outside attacks. Normally, inside attacks are very hard to be detected. As a result of that, those attacks have affected the healthcare infrastructure at a massive scale. The most recent example for this type of attack is the "WannaCry ransomware attack". Those type of inside attacks can not be fully mitigated. However several safety precautions can be made in order to reduce the malicious activity. As a result it might become possible to defend the healthcare system from future attacks. When we consider about the current cyber defense architecture, there is a massive shortfall of defense mechanisms specifically in the healthcare sector.

"Data Breaches" are the most common & the most frequent attack vector that can be experienced in any type of critical infrastructure. This is applicable for many various sectors such as healthcare, communications, oil & gas, power, transportation and finance sector etc. When a particular sector is considered, its different infrastructures are connected with each other. As a result of that when one sector is compromised, it will cause a disruption in the entire infrastructure. Since from the early world war stages, healthcare sector has been a target of the enemy troops. But in the present, it has evolved in to an electronic warfare. With the current technology, cyber attacks are perfectly capable of disrupting the healthcare critical infrastructure in a very stealthy manner. Most of the times those attacks are performed remotely & anonymously. In a global pandemic situation like Covid-19, security compromise in the healthcare sector may cause a massive destructive impact on a entire nation. As the final result, this may cause a very dreadful situation to all the services in a country including the economy.

II. Research Statement (Objectives)

The main objective of this review paper is to identify new methods & techniques in defending the critical infrastructure of healthcare sector from cyber attacks. Usually, the main security of a system consists with multiple layers of security zones. In order to slip between all those security layers, an attacker needs to be a well-talented professional who has expertise in that area. As a result in the modern world, most of the attacks are done anonymously & remotely. When the healthcare sector is concerned, attackers are capable of threatening the entire life of human race.

When compared to other sectors, healthcare sector is clearly exposed for the risk of being attacked easily. The healthcare sector has become so such vulnerable to cyber attacks because it consists with a poorly constructed security infrastructure. Later in this review paper, the greatest threats & vulnerabilities for the healthcare sector and the frequency of those security breaches are going to be addressed. When addressing on those sections, it's very much vital to deep dive on those areas. As it was previously explained, currently the whole world is passing through a global pandemic situation. As a side effect of that, malware & phishing attacks on the healthcare sector have increased rapidly during the past several months. Fake & malicious URLs are being passed in a massive amount, throughout the healthcare sector. Most of the times those attacks are carried out by deceiving the general public that they are already infected with Covid-19. Currently, in most of the countries it has become a trend to develop an app in order to track the real-time progress of the pandemic situation. But most of those mobile apps are injected with malicious codes, which are capable of stealing sensitive information from users.

Following are some of the most common & frequent threats in healthcare sector.

- Data theft for impact
  In here, attackers steal sensitive medical information and release it to 3rd parties.

- Data theft for financial gain
  In here, attackers steal personal sensitive data in order to gain economical benefit out of it.

- Denial of service attacks
  In here, an attacker floods a particular system with excessive amount of requests. As the result, the entire system or network will become unavailable.

- Data corruption
  In here, an attacker corrupts or alters the data intentionally in order to gain personal or political advantage out of it.

- Ransomware
  In here, attackers lock-out users from their devices by making those devices unusable. Then the attackers threaten users demanding money in return.

- Business email compromise
  In here, attackers perform fake communications with users, in order to fraud their money.

- Natural threats
  Rarely, there might be occasions which make the critical infrastructure of healthcare sector vulnerable due to unavoidable, natural threats such as floods, earthquakes, tornadoes, landslides etc.

When the healthcare sector is considered, it is extremely vulnerable to cyber attacks. Having limited resources and improper governance & guidance are some of the main reasons which weaken the critical infrastructure security in the healthcare sector. Additionally, the short supply of cyber security experts in healthcare sector has lead the pathway for devastating consequences. Clearly in the healthcare sector, there is no person responsible for securing its systems and data. According to the analytics report of HIMSS in [1], threats towards the information security in healthcare sector have risen up rapidly during the past several years. Between 2006-2007 time period, it has been recorded that over 1.5 million patient information were exposed due to the data breaches that occurred in various hospitals. However those threats can be either deliberate or accidental. Either way, when it comes to the practical usage of information security systems in healthcare sector, it's less reliable when compared with other systems. Most of the information security systems in hospitals have failed to sustain the confidentiality, integrity and availability.

Preventing data breaches is not an easy task at all. In modern world, healthcare systems are inter-connected with each other in order to exchange information quickly across multiple platforms. Obviously, this has increased the risk of exposing those healthcare systems for data breaches. When the patients' data is stolen, it becomes very hard specially when treating those patients. In past several years lot of data breaches were reported because of loss or stolen devices. In order to prevent any kind of data theft, encrypting the data is very much essential.

Hackers also use social engineering techniques in order to gain access and cripple the medical systems. Insufficient amount of security awareness within medical staff lead the pathway for the attackers to perform social engineering attacks on them. Most of the times, hackers manipulate the medical staff in order to disclose sensitive information of patients such as usernames, passwords, financial data etc. Due to the technological advancement, currently there are huge variety of IoT based medical instruments out there such as remote medical devices, tablets, wireless medical sensor networks (WMSNs) etc.

III. Review of the literature

According to Lavin R. & Harrington M.B in American journal of disaster medicine [2], a critical infrastructure can be simply defined as "systems & assets". This critical infrastructure can be either physical or virtual. Either way, the compromise of those basic infrastructure leads the pathway to create a huge impact on national public health & safety.
According to Lavin R. & Harrington M.B [2], the public healthcare critical infrastructure consists with 3 main components.

- Workforce capacity & competence
- Information & data systems
- Organizational capacity

Additionally, the public healthcare critical infrastructure consists with 10 essential public health services.

- Monitoring health status
- Diagnosing & investigating
- Informing, educating & empowering
- Mobilizing partnerships
- Developing policies & plans
- Enforcing laws & regulations
- Linking people to services and ensuring the provision of otherwise unavailable healthcare
- Ensuring a competent workforce
- Evaluating effectiveness, accessibility & quality
- Researching

A. The importance of public healthcare infrastructure

When it comes to the public healthcare infrastructure, there are considerable amount of threats towards it. The most recent example for this is the Covid-19 global pandemic situation. Such kind of threats have the potential to impact on both general public health & the healthcare infrastructure.
According to Murphy, C. J in "Cyberattacks and the effect on healthcare critical infrastructure" [3], usually the healthcare sector has always been a target for the attackers since from the past. Attackers target this sector mainly because of its value protected healthcare information (PHI). Those information has a huge value specially in the black-market. However when an other sector, such as the financial sector is considered, the black-market value of the stolen data decreases in a much more higher rate due to the shut down & replacement of the bank cards. But when it comes to the healthcare sector, those stolen records can be used by the attackers for multiple purposes.
Usually, those records contain;

- Name of the patient
- Address of the patient
- Social Security Numbrs (SSN)
- Date of Birth (DoB)
- Past medical history of a patient
- Insuarance information

According to Murphy, C. J in "Cyberattacks and the effect on healthcare critical infrastructure" [3], Protected Healthcare Information (PHI) provides attackers with huge set of advantages.

- Identity theft of patients
- Fraud insurance claims
- Requesting for bank loans
- Deploying specific target based attacks

Most of the attackers target the healthcare critical infrastructure in order to manipulate medical equipment & to perform data breaches. It has been recorded that since form 2009, over 155 million Personal Identifiable Information (PII) records were exposed to the general public. When compared to other critical infrastructures, the total loss caused by data breaches in healthcare sector is far more above than the average.
According to Anthony Cuthbertson, *a reporter for Newsweek*, a ransomware attack which took place in Hollywood Presbyterian Medical Center caused a massive commotion in the hospital. It forced the medical center staff to turn back patients & ambulances away and cancel the pre-channeled surgeries. This immense commotion lasted for about 4 days straight until the hospital finally agreed to pay $17,000 in 40 bitcoins as extortion.

B. Why healthcare sector is so vulnerable?

With the past experiences, the attackers or else the threat actors have successfully identified the potential threat areas in healthcare sector. They also discovered new methods to exploit those vulnerabilities. Not only the data & medical equipment, the employees in healthcare sector are also exposed for major risks. In the recent past, it has been recorded that employee records & identities of doctors have been sold out in the dark web with an immense price tag.
Healthcare sector related organizations have become so much vulnerable to cyber attacks due to various reasons. But the main reason behind all those vulnerabilities is the lack of security implementations in its critical infrastructure. However, in present most of the healthcare related organizations have improved their security infrastructure in a massive scale. From 2008 to 2014, over 96.9% of the organizations have moved towards the Electronic Healthcare Records (EHR) systems. Those modern EHR systems were built upon the old infrastructure. However the organizations in the healthcare sector were not prepared properly for such a massive technological advancement. Most of those organizations did not even had a stable funding mechanism or a cyber security aware staff. As a result of this, vulnerabilities in the healthcare infrastructure was clearly exposed to the attackers.
In the past, huge number of people were allowed to access the Protected Healthcare Information (PHI). This included organization's employees, patients and other third party vendors. This particular permission granting contributed massively in

generating new vulnerabilities in healthcare critical infrastructure.
In healthcare sector, a particular medical organization have to deal with other third party vendors very often.

- When purchasing surgery equipment & implants
- When purchasing medicines & drugs
- When upgrading the current medical facilities
- When following marketing strategies

When compared with other sectors in the society, the healthcare sector is also vulnerable for potential attack vectors. The critical infrastructure of healthcare sector always has been a target of cyber criminals, cyber terrorists, script kiddies & hacktivists.

- Usually script kiddies are not able to discover new vulnerabilities by their own. They perform attacks only on the systems which are pre-labled as vulnerable. Most of the time, those script kiddies are not even capable of generating their on malicious software code. However they purchase or trade malicious software codes from professional hackers in order to perform certain attacks on the systems. Although script kiddies are less dangerous, they still have the potential of bringing significant harm to a particular system.

- Cyber criminals usually perform attacks as their profession. Most of the time those cyber criminals expect an enormous economical benefit out of it. Currently there are two types of cyber criminals in the society which are individual hackers & hackers who are part of a network. Most of the time cyber criminals perform well-organized cyber attacks. Usually, there are two main goals that those cyber criminals want to achieve while performing attacks. The first goal is to steal sensitive, critical information & sell them on the dark web with a higher price tag. In order to achieve this particular goal, cyber criminals use special undetectable web-browsers such as TOR browser. The second goal of those cyber criminals is to hold particular systems as hostage by using different kind of ransomware. Ransomware is capable of blocking the users from accessing their own devices. By doing so, cyber criminals get the opportunity to get a huge economical benefit in the form of extortion.

- When it comes to the cyber terrorists, their only goal is to disrupt or destroy a particular organization's critical infrastructure. In present, the most active cyber terrorist group yet identified is the "Cyber Caliphate". However those cyber terrorists assist and train fellow attackers by teaching hacking techniques & various malicious tools.

- When it comes to the hacktivists, they are mostly driven by political parties. Usually those hacktivist groups consist with both script kiddies & professional hackers. Most of the time, hacktivists perform DDoS attacks towards their targets. Additionally, organizations in healthcare sector are the most favourite targets of those hacktivists.

C. Cloud-Based Healthcare System

In modern world, cloud computing has dominated almost all the sectors in the society. Most of the healthcare providers have already adapted for this technology. When it comes to the healthcare sector, there are massive amount of advantages in cloud-based technology.
According to Deng, M. & Petkovic, M. in *"Addressing Security and Privacy Challenges"* [4], here are some of the most highlighted advantages in Cloud-Based healthcare critical infrastructure.

- Scalability
- High efficiency
- Adaptability
- reliability
- Cost reduction
- Resilience

This particular cloud-based healthcare system has contributed massively in improving the quality of delivered healthcare. Unfortunately, there are certain drawbacks which are associated with with cloud computing in healthcare sector. Moving the sensitive & critical patient data from hospitals to clouds may expose those data to the attackers. In some countries, it is illegal to transfer patient records to the cloud without proper explicit consent of patients.
According to Zhang R. & Liu L. in *"Security models and requirements for healthcare application clouds"* [5], in the modern world, most of the medical records are stored in a centralized database in the form of electronic records. For each healthcare provider, there is an Electronic Medical Records (EMRs) system of their own. The process of sharing electronic records between different EMR systems are usually known as Electronic Health Records (EHRs). However, the higher cost & poor reliability are some of the major drawbacks in this EHR systems. As an effective solution, cloud computing helps massively in reducing those costs to a minimal level. Although many people predicted that the cloud technology is going to make a revolutionary change in the healthcare sector, there are some considerably high risks associated with it.
According to Abrar H. & Hussain S. J. in *"Risk analysis of cloud sourcing in healthcare and public health industry"* [6], it has discovered out that there are various security & privacy issues bounded with the cloud based infrastructure in healthcare sector.
As the attackers are aware of the black market value of those patients' data, they always try to breach & steal those data. Specially when transferring & storing the patient records, current security implementations need to be reinforced.

- EHR & EMR systems need to be guarded with proper encryption mechanism

- Enable secure storage facilities for EHR & EMR systems
- Transmission & accessing of data need to be controlled by using proper authorization mechanisms
- Creation & maintenance of EHR & EMR systems should always preserve the authentication, authorization and accounting
- In order to preserve the non-repudiation, end-to-end source verification process should be performed using signatures and certification process

D. Risks associated with medical devices

With the improvement of modern technology, medical information records are now stored in electronic media. However due to the higher value of those information, those electronic storage media have become targets of cyber criminals. According to Lecklider T. in *"Mitigating medical device risk"* [7], the importance of medical devices are rising up at a very higher rate.

Due to high potential risks in the medical devices, manufacturers are asked to follow certain guidelines when manufacturing those medical devices.

- Particular medical device should be estimated with potential risks & vulnerabilities
- Particular device should be estimated with proper risk tolerance level (Risk Appetite)
- What kind of impacts are made due to the vulnerabilities
- Countermeasures to mitigate those vulnerabilities

Additionally, the manufacturers of those devices are asked to share critical security-related information though an Information Sharing Analysis Organization (ISAO). Healthcare sector related medical devices can be called as an "double-edged sword". If an attacker gains access over a critical medical device, it might affect the entire healthcare sector in a very terrible manner. Most of the currently used medical devices are purely based on IoT. Due to the poor security infrastructure, those medical devices are highly exposed for hacking & malware attacks.

According to Kumar P. & Lee H. J. in *"Security issues in healthcare applications using wireless medical sensor networks"* [8], with the improvement of modern technology, it has been possible to monitor the patients using Wireless Medical Sensor Networks (WMSN). These WMSNs are capable of building a reliable communication with the patient, tracking the mobility of the patient & creating energy efficient routing. According to Legaspi J. in *"Exploring the Cybersecurity Measures Healthcare"* [9], WMSNs consist with direct human involvement & usually those are deployed at a small scale. Wireless Medical Sensors are mostly used to closely monitor the physiological state of the patients. Those medical sensors are perfectly capable of sensing a particular patient's vital body signs. After that those sensed data is transmitted into a remote location without any kind of human involvement. Then a doctor can use those records to get an idea about a particular patient's real time health status.

However those kinds of modern technologies in the healthcare sector makes a patient's privacy vulnerable. As a result of that any sort of data leakage may lead the patient to a huge embarrassing situation. Such kind of situation may badly affect on his/her occupation & insurance protection. Making a patient's private information publically available may cause life-threatening risks to a patient. An eavesdropping attacker may use those private information to ruin a particular patient's whole carrier. In order to avoid such kind of incidents it's very much vital to reinforce the security and privacy of those data. Not only that, when the sensed medical data is sent towards the hospital servers, those data can be intercepted by the attackers. An adversary can easily capture those data from wireless channels and there is a possibility of altering those data as the attacker wants. However in order to control such kind of situations, new laws have been established such as Health Insurance Portability and Accountability (HIPAA) act & Health Information Technology for Economic and Clinical Health (HITECH) act. In order to mitigate such kind of attacks, strong cryptographic mechanisms should be used. Although it costs a lot of money, that particular investment is surely going to protect those wireless devices from cyber attacks.

According to Van Deursen N. & Buchanan W. J. in *"Monitoring information security risks within health care"* [10], in order to mitigate those attacks following security & privacy requirements should be fulfilled.

- Confidentiality of data
- Authentication of data
- Integrity of data
- Availability of data
- User authentication
- Key distribution
- Access control
- Freshness of data
- Secure localization
- Forward and backward secrecy
- Communication and computational cost
- Patient permission

E. Impact of Social Engineering Attacks

Social engineering is art of manipulating people in order to get access for the sensitive information. The main goal of such kind of attacks is information gathering. When it comes to the healthcare sector, the attackers trick the medical staff members to gain access over the systems. Such kind of attacks are capable of making a huge impact on the entire healthcare sector. Among all other sectors, social engineering attacks are very common within the healthcare sector.

According to Pollack J. & Ranganathan P. in *"Social Engineering and Its Impacts on Critical Infrastructure"* [11], a typical social engineering attack consists with following 4 steps.

- Identifying the target / Footprinting
- Establishing the trust
- Psychological manipulation

- Execution & achieving the objectives

Cyber criminals use social engineering techniques in order to gain access over the patient information systems. After the attack succeeds, the whole information system converts into an unusable state. Such kind of scenarios needs to be addressed immediately in order to prevent the potential risks for the lives of patients.
According to Priestman W. & Anstis T. in *"Phishing in healthcare organisations"* [12], following are some of the reasons which lead the pathway for social engineering attacks.

- Unawareness
- Carelessness
- Curiosity
- Fear
- Desire
- Doubt
- Empathy and sympathy
- Ignorance

When it comes to the healthcare sector, in most of the time healthcare workers become easy targets of those attackers. Attackers manipulate those healthcare workers in order to disclose sensitive information of patients. According to Mann I. in *"Social engineering techniques and security countermeasures"* [13], following are some of the most common types of social engineering attacks that can be seen in healthcare sector.

- Phishing attacks
- Baiting attacks
- Piggybacking attacks
- Pretexting attacks
- Quid Pro Quo

In the past, there have been incidents of blackmailing hospital staff by locking them out from their systems using ransomware. In order to mitigate such kind of social engineering attacks, the management of the healthcare infrastructure needs to be involved. New mitigation techniques need to be implemented such as constant monitoring & communication. Additionally, the necessary security updates & reminders should be given to the healthcare staff members in a more timely manner. It's very much vital to give a proper training for all the healthcare staff members about mitigating social engineering attacks. Security awareness about social engineering attacks helps greatly in detecting & preventing such kind of attacks in the future.

IV. Future Research

Data breaches are the most frequent & common attack vector in the entire healthcare sector. According to Pandey A. K. & Khan A. I. in *"Key issues in healthcare data integrity: Analysis and recommendations"* [14], it has been predicted that with the rapid development of the software engineering field, in the future, new autonomous software might be developed in order to pre-detect those cyber attacks.

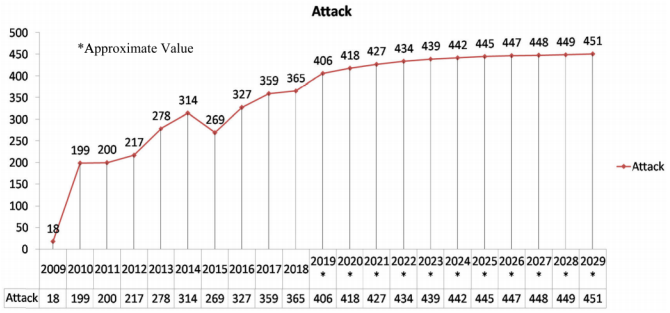

Fig. 1. Forecasting of data breaches

With the assistance of artificial intelligence & machine learning, it might become possible to prevent cyber attacks in healthcare sector in a massive scale.
Healthcare sector can be identified as one of the few sectors that uses big data. As a result of this, blockchain technology is going to become very familiar with the healthcare sector. Although there are certain privacy issues associated with this technology, it is believed that there might be proper solutions for those issues in the future. In blockchain technology, data is stored in a distributed network and each & every node of that network has a copy of relevant medical data. In the future, there might be new expert solutions to manage the privacy of patients' data in a blockchain environment.
According to McLeod A. & Dolezel D. in *"Modeling factors associated with healthcare data breaches"* [15], the maturity of a healthcare organization may affect the total number of security incidents that may occur.
According to Martin G., Martin P. & Hankin C. in *"Cybersecurity and healthcare"* [16], in the year of 2014, more than 300 medical devices were identified as being at high risk level. Due to the poor implementation of security infrastructure, it may bring both financial & reputational risks for the healthcare sector. In order to mitigate those risks it's very much vital to come up with new rules & regulations. Otherwise in the future, patients might become more reluctant to share their data with the healthcare organizations.

V. Conclusion

In this extensive review paper, most of the areas are covered in Critical Infrastructure Security in the Healthcare Sector. According to the analytical data, data breaches are the most common & frequent attack vector. Attackers perform such kind of attacks mainly to gain economical benefit out of it. Usually, cyber attacks in healthcare sector can be divided into 2 main types of attacks; inside attacks & outside attacks. Although in the past only the physical data security was enough, with the improvement of modern attack vectors & tools, in order to protect the patients' data digital or electronic security mechanisms also needed to be implemented. With the massive improvement of the technology, now the attackers have been able to perform attacks remotely & anonymously. The poorly constructed security infrastructure in healthcare sector make their systems

vulnerable to the attackers. Additionally, in the healthcare sector there is no proper governance & guidance mechanism to defend against cyber attacks. When it comes to the data breaches, most of those attacks occur due to the loss of their devices. In order to protect the sensitive information, it's very much vital to use proper encryption mechanisms. The public healthcare infrastructure is very much important for both the medical organization & for the patients.

The healthcare sector has become so much vulnerable for cyber attacks due to various reasons. But the main reason behind all those vulnerabilities is the lack of security implementations in its critical infrastructure. Specially when dealing with 3rd party vendors, it's very much important to follow a industry standard protocol. When it comes to the healthcare sector security, there are different types of threat actors involved in it such as cyber criminals, script kiddies, cyber terrorists etc.

With the gradual improvement of the technology, the healthcare sector has also moved to cloud-based infrastructure. Cloud-Based Healthcare Systems consist with both advantages & disadvantages. However this particular technology has helped greatly in increasing the reliability & privacy of the patients' data. Additionally, the critical infrastructure security in the healthcare sector was affected by social engineering attacks too.

In a nutshell, the current state of the security infrastructure in healthcare sector is not that much appeasable. The whole security infrastructure needs to be reinforced with modern security techniques & solutions.

ACKNOWLEDGEMENT

As the 3rd year 1st semester Cyber Security undergraduates, under the module IE3022 - Applied Information Assurance, we were asked to write a review paper on **"Critical Infrastructure Security in the Healthcare Sector"**. Additionally, we were asked to perform a comprehensive search of the library databases in order to identify at least 15 journal articles that are written on this particular topic. So I would like to make this an opportunity to thank our lecturer Mr. Kanishka Yapa for giving us this wonderful opportunity to enhance our knowledge.

REFERENCES

[1] "Healthcare Information and Management Systems Society (HIMSS)", *Analytics report: security of patient data.* USA: Kroll Fraud Solutions, 2008.

[2] Lavin, R., Harrington, M. B., Agbor-tabi, E., & Erger, N. (2006). Critical infrastructure protection: Why physicians, nurses, and other healthcare professionals need to be involved. American journal of disaster medicine, 1(1), 48-54.

[3] Murphy, C. J. (2017). Healthcare industry held hostage: Cyberattacks and the effect on healthcare critical infrastructure (Doctoral dissertation, Utica College).

[4] Deng, M., Petkovic, M., Nalin, M., & Baroni, I. (2011, July). A Home Healthcare System in the Cloud–Addressing Security and Privacy Challenges. In 2011 IEEE 4th International Conference on Cloud Computing (pp. 549-556). IEEE.

[5] Zhang, R., & Liu, L. (2010, July). Security models and requirements for healthcare application clouds. In 2010 IEEE 3rd International Conference on cloud Computing (pp. 268-275). IEEE.

[6] Abrar, H., Hussain, S. J., Chaudhry, J., Saleem, K., Orgun, M. A., Al-Muhtadi, J., & Valli, C. (2018). Risk analysis of cloud sourcing in healthcare and public health industry. IEEE Access, 6, 19140-19150.

[7] Lecklider, T. (2017). Mitigating medical device risk. EE: Evaluation Engineering, 56(1), 28-29.

[8] Kumar, P., & Lee, H. J. (2012). Security issues in healthcare applications using wireless medical sensor networks: A survey. sensors, 12(1), 55-91.

[9] Legaspi, J. (2019). Exploring the Cybersecurity Measures Healthcare Managers Use to Reduce Patient Endangerment Resulting from Backdoor Intrusions into Medical Devices (Doctoral dissertation, Colorado Technical University).

[10] Van Deursen, N., Buchanan, W. J., & Duff, A. (2013). Monitoring information security risks within health care. computers & security, 37, 31-45.

[11] Pollack, J., & Ranganathan, P. (2018). Social Engineering and Its Impacts on Critical Infrastructure: A Comprehensive Survey. In Proceedings of the International Conference on Security and Management (SAM) (pp. 122-128). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[12] Priestman, W., Anstis, T., Sebire, I. G., Sridharan, S., & Sebire, N. J. (2019). Phishing in healthcare organisations: Threats, mitigation and approaches. BMJ health & care informatics, 26(1).

[13] Mann, I. (2017). Hacking the human: social engineering techniques and security countermeasures. Routledge.

[14] Pandey, A. K., Khan, A. I., Abushark, Y. B., Alam, M. M., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Key issues in healthcare data integrity: Analysis and recommendations. IEEE Access, 8, 40612-40628.

[15] McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. Decision Support Systems, 108, 57-68.

[16] Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we?. Bmj, 358.

AUTHOR PROFILE

H. P. Dilshan Eranda, Cyber Security Undergraduate at Sri Lanka Institute of Information Technology.

Eranda's areas of expertise include **Ethical Hacking, Vulnerability Assessment and Penetration Testing (VAPT), Data Loss Prevention, Firewalls and Risk Assessment.** He is also an blog-post writer in Medium.com. Eranda has a genuine passion towards cyber security. He has performed several real-world penetration testing operations too. He is a self-motivated person who is willing to achieve all the ambitions and dreams in life through strong willpower, commitment, passion and self-confidence. Eranda is naturally talented in soft skills such as leadership, teamwork and resource & time management.