A Review on Cyber Security threats and mitigations in the Healthcare Sector with emphasis on medical internet of things and SDN

Dias L.R.S
department of computer system engineering
sri lanka institute of information technology
malabe sri lanka
IT20076498@my.sliit.lk

***Abstract*— The Internet of Things (IoT) is gaining traction, with There are trillions of gadgets and systems that are wirelessly linked, set to embrace various IoT technologies and share potentially sensitive data in the near future. Wi-Fi and cellular Internet connections are available locally through IPv6 can be used to install IoT devices and connect them to cloud services. The IoT, on the other hand, would allow attackers to discover many susceptible targets and launch assaults since it is a dispersed setting conducive to a free market and a plentiful supply of "big data," as well as unending system interactions. Vulnerabilities and assaults like this might affect systems across critical infrastructures. By playing an essential role in the healthcare business, the Medical Internet of Things (IoMT) is boosting the accuracy, dependability, and manufacturing capabilities of electronic equipment. With the help of academics, the available medical resources and healthcare services are trying to link with one another via the digital healthcare system. The Internet of Medical Things ecosystem is made up of wearable devices, medical devices, sensors, and clinical equipment. The Internet of Medical Things enables a variety of healthcare applications to lower healthcare costs, respond to medical emergencies quickly, and improve the quality of medical care. The dangers and mitigations of cyber security in the healthcare sector, with a focus on medical internet of things, are reviewed in this paper.**

Keywords*— *Internet of Medical Things, Internet of Things, Healthcare, Cyber security, IoT security, IoT risks, security threats and violations.

I. INTRODUCTION

This paper presents a literature review on Cyber Security threats and mitigations in the Healthcare Sector with emphasis on medical internet of things and SDN. Health is described as a state of overall physical, mental, and social well-being. People must live a healthy lifestyle in order to achieve their life goals. People become ill, injuries and crises occur, and hospitals are necessary to diagnose, treat, and manage ailments and diseases properly. [2] The health-care system is divided into many sectors in order to serve many areas of human existence and to cater to a vast population. Since the early twenties, the healthcare system has been progressively shifting toward the technology realm. Everything else, aside from traditional or ayurvedic health methods, is now dependent on technology. More advanced medical equipment is now accessible in hospitals; with this innovative technology, surgeons can execute procedures with a high success rate. [1] [3]

With rise of the covid-19 pandemic modern healthcare systems are supporting at the frontline. Like other sectors healthcare sector is also using computerized systems to manage their work from admitting a patient to a hospital, to critical surgery. These systems are adapting to the modern world, now Internet-of-Things can be seen within the hospital infrastructure. Before the use of IoT hospitals are using web-based systems to provide an effective service to patients. Patients can make an appointment to the doctor that they are willing to get treated by using these systems. Leading hospitals are now using technology to conduct video meetings with doctors and patients. Patients can order their medicine by using a mobile application to their doorstep.

As above mentioned, people are getting benefits from the existing technology in the healthcare sector, while doctors and healthcare workers using the modern technologies to provide better and seamless service to patients. Doctors are performing robot-assisted surgeries to reduce variations in performance. These robot-arms can reach to body or organ places human arm cannot reach. Genomic testing is used to detect and analyze cancers, and to prescribe personalized medicines. Artificial intelligence will improve the precision of diagnosis and therapy. Most of the hospitals and home clinics are using digital records of patients for easy access of data, and there are large scale companies to manage patient and hospital information. Therefore, healthcare systems, databases, mobile applications, theatre equipment etc. are connected to internet[4][1]. Problems are begun to arise with this point. Everything that are connected to the internet are vulnerable to some kind of a cyber-attack. Patient records, hospital digital records, lab reports, chemical or medicine details are listed under sensitive confidential data. Healthcare systems have to protect data while preserving confidentiality, integrity, and availability (CIA triad) as these systems serve life-critical services. [2] [3]

Healthcare is a universal necessity that impacts everyone in societal structure. The healthcare industry is responsible for gathering and maintaining extremely sensitive and personal data while also sharing it with medical personnel, patients, and other organizations. According to internet, cyber-attacks on health systems doubled in 2020. Industry is facing to ransomware, data breaches, DDoS attacks and IoT- based attacks. There is 28% increase in ransomware attacks to hospitals. Attackers are using outdated servers to upload the payload to the system and demanding a ransom to release the information.[1][2][3] Hospitals cannot go ahead on the work without data they want.

According to researchers there is a rise of ransomware attacks with covid-19 pandemic situation. Research found that health care systems are the most attacked and most vulnerable to data breaches. Databases associated with this industry is contained with most confidential information of human life. Patients or customers confidentiality can be damaged by leaking a single document to internet And data breaches by health databases can lead to bio-attacks. Attackers can use the information to carry out a bio-attack on a specific person or on a specific group of people. With the ever-evolving technology everything from tiny smartwatch to large scale production line machine is connected to internet. In health systems, surgery equipment and robots used in operation theatres and many other devices are connected to the internet [6]. Devices that are connected through internet to exchange are IoT devices. E-Health devices such as heart implants, smart fitness trackers and other remote human health monitoring tools are connected to internet for easy management. For healthcare systems, IoT devices are critical[4]. IoT devices generate quantifiable and computable medical information to make healthcare apps easier to use. Easy comes with many vulnerabilities, IoT devices used in health systems are attacked several times, DDoS attacks, snooping attacks and routing attacks are the most common attacks to IoT devices. Attacks on these systems can disrupt the entire process of a hospital.[1][2]

HealthCare Systems are driven to develop in response to technological advancements. Health record digitalization has aided the transformation centered, specialist-focused practices to dispersed, patient-centered care, which is widely recognized as both inevitable and vital. Breach of HCS cyber-security that exposes personal data or information will have a severe impact on facility, with potentially fatal repercussions. Create these elements, taking into account the parameters listed below. Ransomware attacks, hacking of personal medical equipment, and theft of personal medical data are all increasing the cyber-security risk to healthcare.

Because of the tremendous value of personal information, stolen health data are worth more than stolen records from any other [14] business. They may support criminal activities and ease when sold on the dark web. As a result, the hackers will be able to combine employment records for federal employees with sensitive health data, allowing them to target high-value individuals for damage. Despite a surge in cyber-attacks on health organizations throughout the world, the healthcare industry continues to lag behind other industries in terms of its ability to safeguard crucial data. Healthcare cyber-security has been highlighted as a developing health security concern, however there is a lack of knowledge of the danger in the health industry. To combat rising cyber threats, a healthcare cyber-security capabilities strategy is necessary.

When we combine that with IoT, A link to the Internet may improve any electrical equipment, allowing it to become a smart object on Iot. In the healthcare industry, for example, nowadays most medical equipment may use information collected from cyberspace to enhance their fundamental operation and become smarter, more efficient, and economically practical. To link smart devices, the Internet of Things relies on wireless networks and communications. Because of their mobility needs, wireless communications are required, as well as information via IOT AI devices, sensors that collect linked with health information can be gathered and analyzed with the goal of enhancing our everyday lives, smart device connections could potentially disclose personal healthcare data.[1] Whenever any patient wears/wear AI sensor which connects to either a different gadget at a specified location, connection betwixt the two devices might be used for nefarious purposes like tracking the patient's activity. Despite the fact that healthcare professionals such as physicians, nurses, and paramedics are typically trusted and thought to access and distribute patient information as intended, there is always the possibility that unauthorized parties will obtain the information. [2][3] While real-time patient monitoring can aid find when a patient's blood pressure is high or when he or she is at risk of a heart-failure, the same data can possibly seize as well and expose other information that makes when patient was in peril with death. With so many gadgets becoming networked, the Internet of Things poses some significant concerns. More systems are becoming linked and complex in essential contexts universal health care, for example. The hazards in IoT-based critical systems are increasing, and any disruption or corruption might result in costly damage or life-threatening issues.[1][2]

II. Research statement

This paper reviews some attacks on healthcare systems, attack vectors, and countermeasures that have raised concerns about safety in the healthcare sector and how vulnerable they are to attacks by hackers or other attackers, theft actors in the field, examples of attacks, and how they occurred. This evaluation also supplies a jargon which needs clarification. In addition, the analysis would describe solutions recommended by the research paper's experts, along with facts or knowledge on proposed solutions, and whether the mitigation of the vulnerability was possible. Moreover, valuable information on the subject of research cannot, in the research selected for review, be provided, the differences found in different studies are explained in this review and the review also includes personal recommendations for the issues raised.

III. Literature Review

A. Healthcare and Cybersecurity challenges

Medical providers are taking use of the Internet's networked nature and seek to use it and distributed computing to assist their customers/patients to the fullest extent possible. Healthcare providers are increasingly web connected, have a plethora of technologies to manage, and are vulnerable to a growing variety of security risks. Vulnerabilities in a system, unauthorized access, an insider executing unauthorized operations, or natural calamities earthquakes, flooding, and storms, to name a few, and lightning are all potential threats. External security risks and internal security threats are the two categories of attacks. Denial of service (DoS) assaults, remote brute-force attacks, and man-in-the-middle attacks are examples of external security risks. Internal security concerns include password snooping, Trojan horses, and data manipulation.[6]seven [] Such assaults pose a direct danger to the metadata of a medicinal treatment supplier' confidentiality, integrity, and availability. The Security Rules and Procedures of the Health Insurance Portability and Accountability Act (HIPAA) have offered a variety of measures to reduce such dangers and hazards. Web-based healthcare is on the increase, apps As a result, a plethora of new vulnerabilities

to patient data security have emerged. Malware and illegal operations, particularly those aimed at medical identity theft and healthcare fraud, constitute a significant danger to the safety of electronic patient records.[8][9][5]

Figure 1 depicts another conventional hospital facility service backed by N3 NHS network services, as well as linkages to other cyberspace entities such as patients, NHS employees, and social media users. Maintaining the safety of patients, linked devices, and hospital systems, as well as keeping a resilient operating environment in the face of such threats, is critical. As a result, cyber security will be crucial creation of secure healthcare services and also A significant priority is to improve patient care. for the healthcare sector, and it is a critical part of NHS changes. Doctors and nurses, for example, require quick and simple access to patient details via specific Web and mobile applications.[5][6]

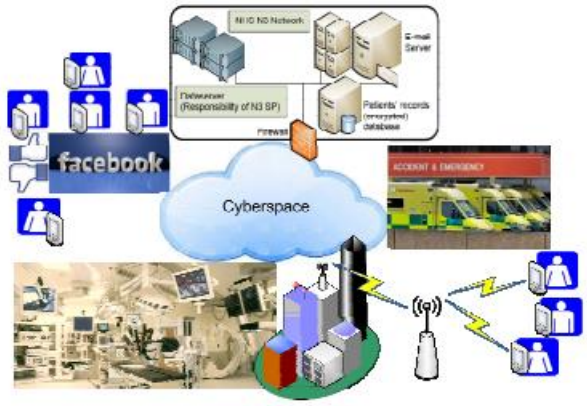

Figure 1

Healthcare Information (EPHI). Furthermore, the widespread use of mobile smartphones has created an atmosphere where patients' wireless conversations and emails from healthcare professionals can be intercepted. In terms of access to patients' files, such as legitimate diagnostic and treatment information, healthcare service providers' lack of proper procedures and security measures offer a security risk. Such issues may have a considerable influence on patients and their ability to take their medications and therapies properly.

With permitted the ability to connect to the N3 infrastructure, the network is designed to assure data security, integrity, and availability. Physical and organizational security methods, as well as the adoption of policies and procedures to restrict user behavior, have been put in place to reduce the possibility of data being intercepted.

B. Healthcare Security issues

Patients cannot easily contact their bank to report the incidence, as they can with online credit card assaults. If patients' medical records are revealed or manipulated, cyber-attacks against healthcare might be fatal. According to cyber security experts, the healthcare industry will be the next large-scale target for cyber-attacks. Since the HITECH Act required the US Department of Health and Human Services' Office for Civil Rights to begin supplying healthcare data breach information on its website, more significant healthcare data breaches were recorded in 2020 than in any previous year. Healthcare data breaches involving five hundred or more records were reported at a rate of 1.76 per day in 2020. [10][7][5]

In terms of the quantity of leaked healthcare records, 2020 was the third worst year, with 29,298,012 records recorded as having been exposed or improperly shared. While this is a concerning number of records, it is down 29.71 percent from the previous year. Since October 2009, there have been 3,705 recorded data breaches of five hundred or more records, resulting in 266.78 million healthcare records being exposed. [6][7][4]

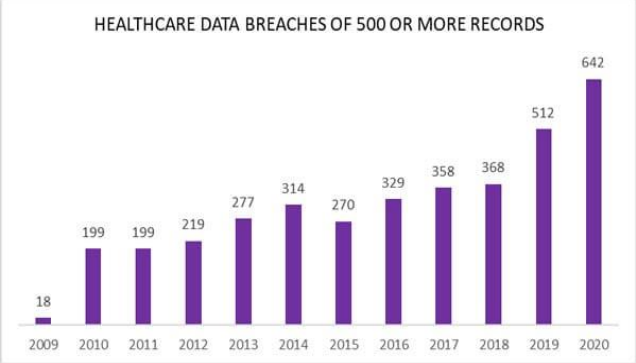

Figure 2

- Since October 2009, 78 million healthcare records have been compromised.
- In 2020, 642 healthcare data breaches involving five hundred or more records were recorded.
- More than ten million data were exposed in one breach, while more than 100K records were exposed in sixty-three others.
- Each day in 2020, 1.76 data breaches involving five hundred or more healthcare records were recorded.
- More than twenty-nine million healthcare records were compromised in 2020.
- Sixty-seven percent of data breaches, and 92 percent of compromised records were caused by hacking/IT mishaps.
- Since October 2009, 3,705 data breaches involving five hundred or more records have been recorded.
- Since 2014, number of healthcare data breaches has more than doubled. [8]

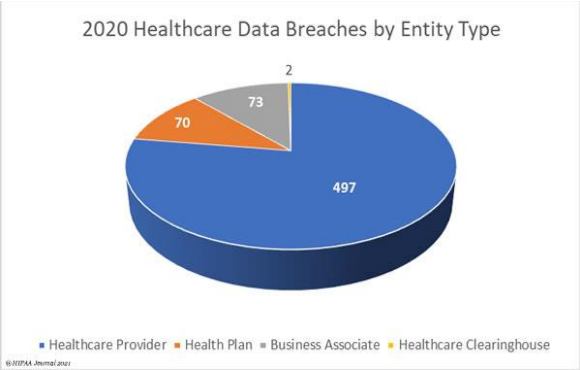

Figure 3

The pie chart below depicts the number of HIPAA-covered companies affected by data breaches of five hundred or more records. With 497 reported in all, there were seventy-three data breaches reported by business associates. In many situations, the breach occurred at the business associate's location. Business associates took part in 258 of the year's breaches, accounting for 40.19 percent of all breaches. Health plans reported seventy breaches, while healthcare clearinghouses reported two breaches.[6][5][4][7]

The researchers came to the conclusion that a more efficient system for detecting or preventing invasion is needed, one that can work with honey spots with dynamic shadows. However, zero-day attacks and vulnerabilities are thought to be the biggest issues still facing the Internet of Medical Things.[7][8][6]

The Internet of Medical Things security assessment method recommends a set of assessment attributes that includes all of the necessary security safeguards. This enables medical internet of things adopters to choose and enforce security in Internet of Medical Things solutions depending on their security goals, which may be changed in a different circumstance. The Internet of Medical Things Security Assessment Framework's uniqueness lies in their capacity to adapt to new technologies as they emerge, as well as the granularity and standard compliance that they provide.so there are circumstances where the system administrators are solely accountable for security choices, but this job provides a good chance for stakeholders to get practical firsthand knowledge of the competitive environment world of On the Internet of Medical Things, there is a lack of security. Key stakeholders are allowed to learn about the hazards connected with medical devices, and they may use the best practices to mitigate those risks and make better judgments based.[8][9][6]

In 2018, They a model was investigated with cryptography and better privacy mechanism that is encoded with authentication. The security issues of the Internet of Medical things can be solved with this paradigm (IoMST). Real-time security and privacy are also major concerns for the Internet of Medical Smart things. The study presents a run-length encoding approach, which was followed by encryption with a rotating key in the patient's system, and the data was decrepit with a rotating key and then decoded with the decoding run-length technique in the physician's system. The patient's digital signature ensures the integrity of the record. and the research might be focused on constructing a Health shield that can and will gather all statistics through the Internet of Medical Sensible Devices' sensing devices and a system that can encrypt data making use of the synchronization method. When the number of sensors in our system is raised, it may be used to solve big data challenges. After that, a personal blockchain of the patient's health record may be implemented. [5][6][7]

CRubi and GRondim (2019) discovered a platform that automatically generates data for OLAP applications via automated recording, ensuring the patient's privacy. The use of the usage of a healthcare repository made data mining easier thanks to the file structure, extraction of knowledge methodologies, and machine learning training of resampled highly automated recording. A development framework was created for "medical IOT" devices, the gateway, and the fog server, allowing for the integration of added platform sensors, the extension of AE functionality at the entry point, and the implementation of new protocols.[9][10][11][5]

C. Case examples of Healthcare security breaches

1. Lukas Krankenhaus Neuss (Germany)

With 527 beds and 1300 personnel, Lukas Krankenhaus Neuss is a public hospital in Germany, founded in 1911. Employees As a result of a “ransomware” attack that was conducted using a social-engineering tactic in February 2016, I received a variety of error messages. here the hospital reacted by shutting down servers and computer systems in order to inspect and sanitize the systems that had been infiltrated. Staff continued to work using pen, paper, and fax machines in the meanwhile, although high-risk processes had to be postponed. Officials in the area suggested contacting the attackers, but no attempt has been undertaken. Although the hospital claimed that a backup mechanism was supported up to date and that just. A There is a a stack of handwritten documents from before the computer systems were installed. were down will eventually need to be connected with the rest of the EHR, despite the fact that just a few hours of data were lost. According to a hospital representative, it will take a few months for the hospital's workflow to return to normal. so, there was no sign of any compromise of patient data.[11][12]

2. The South-eastern Norway regional health authority (Norway)

This South-East Norway Regional Health Authority (South-East RHF) was founded in 2002 alongside three other regional authority as a regional organization run by the government of specialized hospitals and healthcare services. The PHI and data of 2.8 million individuals (more than half of Norway's population) were hacked in January 2018, according to the South-East RHF. The assault occurred before the firm could take security measures to

decrease the dangers posed by Windows XP, as well as a strategy to phase it out. [11][13][9]

3. Hancock regional hospital (The United States)

So called virus SamSam has launched a ransomware assault against Hancock Regional in January. The assault was directed at a server in their emergency IT backup system, propagated via an electronic link between the backup location, which was miles away from the main campus, and the hospital's server farm. Except for backup files for electronic medical records, it was eventually decided the fact that such hackers had irreversibly damaged reliable backup records' aspects from several systems. The Assault Microsoft's Remote Access Protocol was used to conduct the investigation as an access hackers get access to the server used a hardware vendor's administrator account to launch the attack, according to investigators. just about all network and personal computers control systems at the hospital were shut down by the facility's IT department. After the incident. Despite this, hospital operations continued as usual within regular downtime protocols. The hospital was not shut down, and no patients were diverted. The hospital paid the ransom after the hackers wanted four Bitcoins (55,000, USD). All IT personnel subsequently dedicated the very next three to four days decrypting data and attempting to recover them to restore normal operation to the system. They discovered no sign of compromised patient data.[9][7][8]

D. Iot based healthcare cyber-security

Ppatient is at home or in the hospital, Hospital systems are linked to internet healthcare apps allow for the sharing of patient-specific data and health information. As part of the healthcare process, sensor devices in healthcare attached to Blood pressure and heartbeats are monitored by patients, and temperature, track their activity and behavior for the purpose of communicate data to hospital systems. Weak authentication measures might be used by an attacker to obtain access to critical systems that is not allowed. This might enable the attacker to not only disable various hospital systems and get illegal access to critical data, and yet rather to find a means to get to the sensing devices and target victims. A tampered sensor linked to a patient might have disastrous repercussions, and the ramifications of such a security breach could grow to the point where the patient's life is lost. As a result, such equipment must be kept safe and secure at all times. [8][9][10]

Medical sensors in the IoT were meant to gather data on a patient's state in real-time, and hospitals use them. They use that information to aid their patients. It poses a dilemma new risk may arise. Because of its unknown range of features, the Internet of Things as an Emerging Technology will face several security issues. It is difficult to say exactly what makes the Internet of Things smart. This illustrates the difficulty of how security can be done successfully without finding what features the procedure should have, or when or not the system should have may alter on the fly from a security standpoint. The main issue is that current IT security methods may not be adequate to manage future IoT security concerns. Patients' contacts with various gadgets as well as involvement in the health and care system are seen as an uncontrollable source of hazard in the IoT. It appears hard to predict all of the consequences of a potentially harmful human behavior interacting with a highly automated real-time technology. [11][12][13]

The IoT systems auto record screen flow, or time spent in App engagement' a variety of strategies and crashes and procedures are available.[20] The Google Statistics (GA) platform may be used to report on IoT analytics and patient interaction with their surroundings. Allowing system designers to use GA to buy insight on the use and traffic of their IoT applications achieves this. Monitoring patient traits and behavior, use data, and application performance, as well as analyzing usage trends, are all part of this process. GA might also be used to report device defects and system interface failures. Able to monitor IoT things like sensors may be time demanding and resource costly.[14][15]

E. IoT critical infrastructure in HC

Data networks, Control systems, Device sensors, and are used extensively in today's businesses and essential infrastructures. Growing availability of digital services and operations in many industries has resulted in a rise in the number and types of threats and harmful behavior. As threats targeting many infrastructures have grown in popularity, such assaults have become more widespread.[22][21][19] Failure to manage such vulnerabilities across all areas of infrastructure systems might have major consequences for organizations in general, and healthcare service providers in instance. Security breaches and dangers to a variety of systems, such as power generating systems, banking and healthcare services networks, telecom networks have increased significantly in recent years, according to the security community [17][18][20]. Emerging security threats and breaches have been detected in recent years, and they have had a detrimental influence on vital industrial services and infrastructure. Energy and power outages, system failures, and dangerous medical incidents are all examples of cyber security hazards. The rise of critical infrastructure services in the twenty-first century will be aided by recent breakthroughs in the field of infrastructure systems security.[19]

Against the ever-changing cyber threats, IoT critical industrial systems must keep operating environments secure, robust, and safe. All of that is done to keep personnel, industrial assets, and the communities they serve safe. As a result, all organizations involved in running, creating, keeping, and constructing essential IoT infrastructure and systems face a difficult challenge in controlling cyber security threats. A remote attacker may control medical equipment if malware gained illegal entry into a hospital network section hosting a patient monitoring system. The loss of human life might be caused by a hacked IoT sensor in a medical system network. The above means that key IoT systems must keep the operating environment safe, robust, and safe in the face of ever-changing cybersecurity assaults. This is done to keep patients, medical

assets, and the communities they serve safe. Simply applying cyber security to essential IoT systems like healthcare systems is becoming a difficult challenge, but one that is critical to the company's success. Another major element in the rise of crucial IoT operations and services is recent improvements in the disciplines of industrial IoT system security, such as software security, An PLC sensor of security and intrusion detection and prevention and embedded systems security.[18][19][15]

F. SDN in the HC

Manual setup of networking equipment, such as switches and routers is required in conventional networking design. Because of the emergence of new traffic patterns due to the growing popularity of applications in IoT, M2M, mobile and edge computing, escalation of 5G traffic, evolving WAN requirements, and other internet-based applications, this traditional method of networking is deemed incapable of handling the ever-increasing demands for high network QoS and performance. Because of the changing traffic patterns on the network as a result of node mobility, network resource allocation must be flexible while preserving network QoS and performance to the needed standards set. Many networking platforms and businesses are using SDN to meet the ever-changing network demands.[11][20][21] As compared to conventional networks, where network equipment, such as routers and switches must be manually set, the network controller in SDN may be designed and configured to adapt to changes in the communication network, such as traffic load and network architecture. H-IoT networks are vulnerable to security assaults, just like any other network. The network controller in SDN-based H-IoT can become a single point of attack, bringing the entire network down.[15][16][17] As a result, in order to secure an SDN-based H-IoT network, the controller must be secured first. Solutions that can offer dynamic access control to the SDN network controller are necessary to safeguard it from malicious applications and traffic. At the network controller, it is also crucial to integrate solutions for a secure control communication layer, authentication, authorization, and accounting (AAA), API security, logging/security audit service, and resource monitoring.

Figure 1 shows an example of an SDN-based H-IoT system. Following are the three planes that make up the system.

The plane of data

Network devices and equipment used to send data over the network make up the data plane. Data is collected from sensors and other IoT devices via wireless or wired network infrastructure, as shown in Figure 1.

The Plane of control

The decision-making plane is the control plane. The network controller, which has the logic developed for traffic control such as routing, load balancing, and traffic engineering, is the core entity of this plane.

The plane of application

All of the healthcare-related apps that run with H-IoT data are shown in Figure 1's application plane. The receiving apps that collect data from the patient make up the application plane. This information is used to diagnose problems, do analytics, produce statistics, and make informed decisions. [19][18] The decisions or messages made can be communicated back to the patient via the cloud and network controller, as shown in Figure 1.

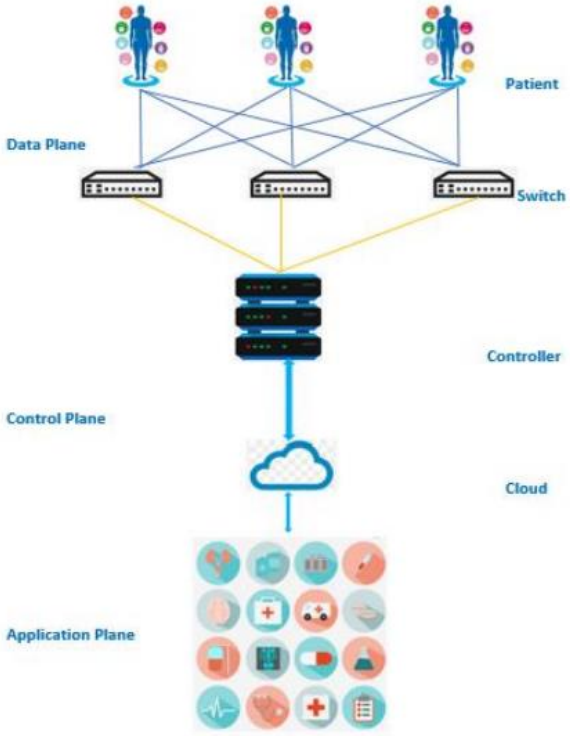

Figure 4

G. Attack vectors and mitigations

1) Vulnerability management, patch management: The detection, Management of susceptibility and exposure includes assessing and mitigating IT vulnerabilities. This risk evaluation is, in most situations, extremely difficult. Patch management is one of the phases toward remediation or mitigation, which might be hampered by a health facility's requirement to operate 24 hours a day, 7 days a week. Patching techniques rely on risk analysis to balance the sensitivity of data on the server with the vulnerability of an enterprise's vital services or assets to an exploit. Organizations should continuously seek for vulnerabilities in their systems and use penetration testing to ensure ongoing vulnerability management. Early detection can assist to lessen the chance of being exposed to a security issue. Without putting too much focus on zero-day vulnerabilities, vulnerability detection should be followed by configuration hardening or patching operations. According to Gartner analysts, 99 percent of exploits are based on flaws that have been known to security and IT professionals for more than years. Organizations should take such results into account when prioritizing the remediation of various risks.[19][20][16]

2) Multifactor administrative support authentication and administrative support executive powers- The dangers of

extending users with administrative privileges in health and wellbeing care institutions are enormous. Per the Privileged Account Exploitation by CyberSheath's APT study, the great majority of large-scale assaults that resulted in considerable damage and costs were started by compromising such an extremely protected identity, such as one belonging to a third-party service even in January 2018. According to a survey, 70 percent of computer-related criminal behavior is caused by unhappy employees. Organizations should reduce the risk of such attacks by regularly monitoring user account lifecycles and removing client and user certificates when they are no longer in use.

IV. Future research

Cyber-attacks are happening every day, zero-day attacks and an zero-day vulnerability count is increasing. Therefore, there must be a comprehensive security strategy for future attacks but unfortunately attack technologies are also evolving with technology. According to majority of researches, Artificial intelligence will use in future than before to help to protect the healthcare systems in different aspects. Information security laws, governance and compliance techniques must take into consideration in healthcare systems. Law enforcement agencies and government laws about data theft are inadequate to address for a data breach or to a device-based attack. Bring Your Own Device (BYOD) is emerging in the healthcare sector as other sectors. Securing devices with multi-factor authentication and encouraging healthcare workers to use biometric authentications to minimize the traditional Bring Your Own Device (BYOD) related attacks. Proactive protections method must increase, using blockchain technology and secure cloud containers to store sensitive information. Maintaining storage backups in separate physical locations and gaining the service from a reputed third-party technology provider is recommended.

V. conclusion

Cyber-attacks cannot be stopped completely, but organizations, institutions, companies can take necessary actions to mitigate, avoid, defer, or transfer risks. Organizations have to be ready for any type of cyber-attack. The Healthcare sector is the most vulnerable sector to data breaches. And it was proved by the series of attacks towards the healthcare systems. Blackbaud incident shows the importance of medical records than financial records. Therefore, there should be a security plan to overcome these attacks. Encrypting the sensitive data is a safety precaution, and conducting awareness sessions to persons at healthcare about the phishing emails, social engineering attacks, company security policies, etc. As technological impact companies or hospitals have to consider more about the security patches and software updates. Next the biggest attack to the healthcare system is attack on medical devices. Almost all the devices connected to the internet is vulnerable to attacks, heart rate measuring devices, artificial implants and life-critical devices are a part of health eco-system. The Internet of Things based attacks are the newest trend in cyber-attacks, therefore security of the physical devices is also important to keep the stability of the healthcare sector.

Using Virtual Private Networks (VPN) and strengthening the security of Bring Your Own Device atmosphere are possible key solutions to overcome from those attacks. Hospitals including entire healthcare sector can be protected by cyber-attacks by implementing correct security measures to correct places. As frightening as today's cybersecurity threats to healthcare infrastructure are, the scariest of all cyber threats could still be on the horizon. But several of them are not precisely registered since it is less relevant to researchers to study. This is a major complication for researchers. As a result, these vulnerabilities must be further investigated and reported so that other researchers can learn more about the HPH sector and its security vulnerabilities. The areas in question and accepted standards are still under progress, however, and have not been accurately assessed in observation studies. In cyber-physical networks, technical considerations are combined with an engineering perspective.

Acknowledgment

I am grateful to Mr. Kanishka Yapa, The Faculty of Computing, Sri Lanka Institute of Information Technology, whose expertise, understanding, guidance and immense support made it possible to me to work on this topic. Big thank you to my colleagues for being a source of motivation to make my work a success. I am thankful to all my family members for keeping their faith in me and urged to me to do better in my life goals.

References

[1] *Arxiv.org*, 2022. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/2009/2009.05394.pdf. [Accessed: 28- Mar- 2022]

[2]2022. [Online]. Available: https://www.researchgate.net/publication/327888469_Effective_Features_to_Classify_Ovarian_Cancer_Data_in_Internet_of_Medical_Things. [Accessed: 28- Mar- 2022]

[3]2022. [Online]. Available: https://www.researchgate.net/publication/328671564_A_secure_real-time_internet_of_medical_smart_things_IOMST. [Accessed: 28- Mar- 2022]

[4] *Hal.archives-ouvertes.fr*, 2022. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01836236/document. [Accessed: 28- Mar- 2022]

[5] *Arxiv.org*, 2022. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1805/1805.11011.pdf. [Accessed: 28- Mar- 2022]

[6]2022. [Online]. Available: https://arakmu.ac.ir/file/download/page/1612245058-1.pdf. [Accessed: 28- Mar- 2022]

[7]"Towards understanding cybersecurity capability in Australian healthcare organizations: a systematic review of contemporary trends, threats and mitigation", *Taylor & Francis*, 2022. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/02684527.2020.1752459. [Accessed: 28- Mar- 2022]

[8]"Cybersecurity Indexes for eHealth | Proceedings of the Australasian Computer Science Week Multiconference", *ACM Other conferences*, 2022. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3290688.3290721. [Accessed: 28- Mar- 2022]

[9]2022. [Online]. Available: https://www.researchgate.net/publication/322876579_Internet_of_Things_Security_A_Review_of_Risks_and_Threats_to_Healthcare_Sector. [Accessed: 28- Mar- 2022]

[10]2022. [Online]. Available: https://www.researchgate.net/publication/322876579_Internet_of_Things_Security_A_Review_of_Risks_and_Threats_to_Healthcare_Sector. [Accessed: 28- Mar- 2022]

[11]"The Trespass Project | Experimenting with Incentives: Security in Pilots for Future Grids", *Trespass-project.eu*, 2022. [Online]. Available: http://www.trespass-project.eu/node/176. [Accessed: 28- Mar- 2022]

[12]"Health Care Information Systems", *Google Books*, 2022. [Online]. Available: https://books.google.lk/books?id=rilQEAAAQBAJ&pg=PA285&lpg=PA285&dq=HHS,+(2016).+https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf+%5Baccessed+on+15th+Jan,+2016%5D&source=bl&ots=uVMU4VOYhY&sig=ACfU3U0eyMeDBaF2p-_e6zwnQQG-swDVSQ&hl=en&sa=X&ved=2ahUKEwiCr9zgjun2AhURRt4KHTWJBUUQ6AF6BAgCEAM#v=onepage&q=HHS%2C%20(2016).%20https%3A%2F%2Focrportal.hhs.gov%2Focr%2Fbreach%2Fbreach_report.jsf%20%5Baccessed%20on%2015th%20Jan%2C%202016%5D&f=false. [Accessed: 28- Mar- 2022]

[13]"IEEE Xplore Full-Text PDF:", *Ieeexplore.ieee.org*, 2022. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7274428. [Accessed: 28- Mar- 2022]

[14] *Scholarworks.sjsu.edu*, 2022. [Online]. Available: https://scholarworks.sjsu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1300&context=etd_projects. [Accessed: 28- Mar- 2022]

[15]2022. [Online]. Available: https://www.researchgate.net/publication/271729003_Cloud_Security_Auditing_Challenges_and_Emerging_Approaches. [Accessed: 28- Mar- 2022]

[16]"Internet of Things (IoT) Databases", *MongoDB*, 2022. [Online]. Available: https://www.mongodb.com/use-cases/internet-of-things. [Accessed: 28- Mar- 2022]

[17] L. University, "Repurposing web analytics to support the IoT - Research Portal | Lancaster University", *Research.lancs.ac.uk*, 2022. [Online]. Available: http://www.research.lancs.ac.uk/portal/en/publications/-(4b49f4e5-632c-4db4-9c14-e58440c71956).html. [Accessed: 28- Mar- 2022]

[18]2022. [Online]. Available: https://www.researchgate.net/publication/295812759_A_New_MAC_Address_Spoofing_Detection_Technique_Based_on_Random_Forests. [Accessed: 28- Mar- 2022]

[19] 2022. [Online]. Available: https://www.semanticscholar.org/paper/Securely-Making-%22Things%22-Right-Kolias-Stavrou/aa32eb2b0569e5d597dc4f9c680aaae914f84f64. [Accessed: 29- Mar- 2022]

[20]2022. [Online]. Available: https://www.semanticscholar.org/paper/Cybersecurity-in-healthcare%3A-A-narrative-review-of-Coventry-Branley/925ad0ef41b6ec5f4f72390b5002444be3a1b247. [Accessed: 29- Mar- 2022]

[21]Enisa.europa.eu, 2021. [Online]. Available: https://www.enisa.europa.eu/topics/criticalinformationinfrastructures-and-services/health. [Accessed: 17- May- 2022].

[22]https://www.cisa.gov/sites/default/files/publicatio ns/nipp-ssp-healthcare-public-health-2015-508.pdf. 2022.

[23] https://www.mdpi.com/2071-1050/12/17/7002. 2022.

[24]E. Biasing, "Healthcare Critical Infrastructures Protection and Cybersecurity in the EU: Regulatory Challenges and Opportunities", SSRN Electronic Journal, 2022. Available: 10.2139/ssrn.3827114.

[25] https://arxiv.org/abs/1904.01551. 2022.

[26] https://www.phe.gov/Preparedness/planning/cip/Pages/default.aspx. 2022.

[27] https://www.aha.org/system/files/2017- 12/ahaprimer-cyberandhosp.pdf. 2022

[28]"Software-Defined Industrial Internet of Things | Wireless Communications & Mobile Computing", *Wireless Communications & Mobile Computing*, 2022. [Online]. Available: https://dl.acm.org/doi/10.1155/2019/7947638. [Accessed: 29- Mar- 2022]

[29]"Virtualization In Cloud Computing", *Online essay writing service*, 2022. [Online]. Available: https://sourceessay.com/virtualization-in-cloud-computing-cloud-computing-assignment-help/. [Accessed: 29- Mar- 2022]

[30]"Cloud Management using Network Function Virtualization to Reduce CAPEX and OPEX", *Research*, 2022. [Online]. Available: https://research.msruas.ac.in/publications/cloud-management-using-network-function-virtualization-to-reduce-capex-and-opex. [Accessed: 29- Mar- 2022]

[31]*Scholarworks.uark.edu*, 2022. [Online]. Available: https://scholarworks.uark.edu/cgi/viewcontent.cgi?article=2365&context=etd. [Accessed: 29- Mar- 2022]

[32]*Arxiv.org*, 2022. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1908/1908.00666.pdf. [Accessed: 29- Mar- 2022]

[33]L. Coventry and D. Brinley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward", *Academia.edu*, 2022. [Online]. Available: https://www.academia.edu/48662174/Cybersecurity_in_healthcare_A_narrative_review_of_trends_threats_and_ways_forward. [Accessed: 29- Mar- 2022]

[34]2022. [Online]. Available: https://scholar.google.dk/citations?view_op=view_citation&hl=da&user=8Rwg4pkAAAAJ&citation_for_view=8Rwg4pkAAAAJ:qxL8FJ1GzNcC. [Accessed: 29- Mar- 2022]

[35]2022. [Online]. Available: https://journals.sagepub.com/doi/abs/10.1177/1073110519898046. [Accessed: 29- Mar- 2022]

AUTHOR PROFILE

Dias L.R.S, BSc (Hons), in Information Technology specialized in Cyber Security, future Graduate. Her passion and talent for aligning security architecture, plans, controls, processes, policies, and procedures with security standards and operational goals brought him to the SLIIT, where she is working on his BSc in cybersecurity. She has always been fascinated by the area cyber security and its interaction with various sectors. She who is Hardworking undergraduate student with excellent communication, planning, and organizational skills Highly organized, responsible, and initiative taking to remain on track, fulfill tight deadlines, and achieve targets. Strong analytical and organizational skills within the IT industry.

In addition to academic studies, she accomplished certificated such as, A web audit, Web Audit (Website Vulnerability Assessment on selected domain) done in Kali Linux using Tools: Burp Suite | Netsparker | Nikto | Nessus |Nmap | DotDotPwn | Wafw00f | Dtect | SSLyze, Report on Integrating AI in Cybersecurity along with its latest Developments This report discusses all the rising AI innovations and Future trends while integrating AI in cybersecurity in detail. Android device exploitation using Metasploit framework The method I used for the exploitation is android 86 version. Because this vulnerability was only available in android 86.