Cybersecurity Threats and mitigations in the Healthcare Sector with emphasis on Medical Internet of Things and SDN

IT20021870 – Dilshan K.N
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology,
New Kandy Rd, Malabe, Sri Lanka
it20021870@my.sliit.lk

Abstract — **Cyber security has become the front of mind for enterprises throughout every sector in the recent past. Due to the pandemics, many organizations shifted to working from home, then the points of attack surfaces continued to be developed into personal devices, homes, and anywhere else vital information was being accessible. Same as the Internet of Things (IoT) became a vital aspect of industry functioning during the past several years. IoT systems have experienced an amazing increase in sectors such as healthcare, agriculture, supply chain, smart energy, building, and industrial automation, and connected cars. With the help of IoT, the healthcare and global health sector, prospered. Normally, the healthcare sector is a large and broad sector that facilitates an assortment of commodities and services that are crucial to the safety, health, and well-being of people. However, healthcare cyberattacks have become a massive concern for a while because of several aspects. Conventional security strategies, in which security is implemented as an optional extra and as a "patch" against common threats, are insufficient. New generation IoT difficulties will, without a doubt, need an innovative degree of security through the design phase of the project, in which dangers are handled in advance and IoT devices learn to dynamically respond to changing threats. To provide IoT devices with both tunability and intelligence, software-defined networking [SDN] and machine learning will be necessary.**

Keywords: Cybersecurity, Healthcare sector, Cyberattack, Internet of Things [IoT], Software Defined Network [SDN].

I. INTRODUCTION

In the previous few years, there seems to be huge growth in the amount of Internet of Things (IoT) devices. There will be over 25 Billion interconnected IoT devices in 2020 with a rise of about 300 million new devices every month [1]. IoT network comprises sensors, appliances, and other things able to interact without human participation and these devices are easily recognized, have advanced information processing and decision-making capabilities, and have networking capabilities that allow them to communicate via the Internet. The Wireless Sensor Networks (WSN) provide the backbone for the IoT ecosystem to merge with different devices, networks, and things. When expressing the IoT-enabled devices through the healthcare sector, they are redefining patient-medical professional interaction and transforming the healthcare industry. Patients and their families, as well as the Internet of Things in healthcare benefits hospitals, physicians, and insurance companies. Fitness bands, pulse oximeters, glucometers, blood pressure monitors, and heart rate monitors are examples of wearable medical equipment that allow for continuous monitoring of a specific patient's health status. Physicians can access a patient’s health remotely and suggest appropriate possible treatment depending on the patient’s location [1]. People can use fitness tracking monitoring devices to keep track of their fitness levels and calorie consumption. Users can track the variables over time and take appropriate actions or precautions by connecting these devices to the cloud. In hospitals, IoT is used not only to monitor patients' health and location but also to track the location and operation of medical equipment equipped with sensors in real-time.

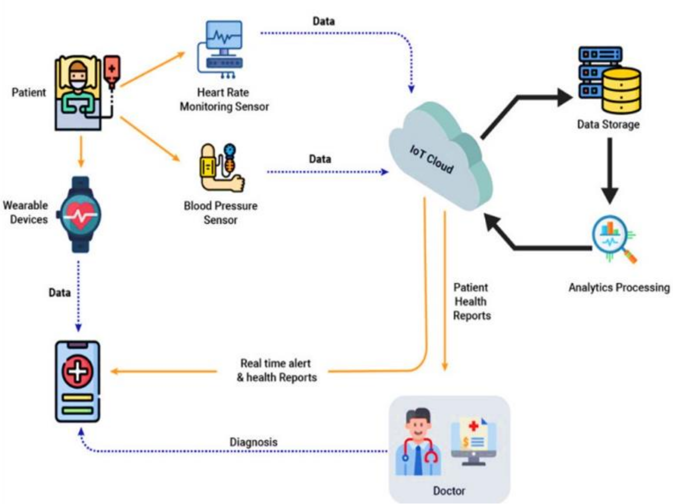


Figure 1.1

With the immense of connecting IoT devices comes an overall increase in network traffic, needing high network bandwidth, compute, and storage. IoT devices, which are largely made up of mobile nodes, often communicate over wireless networks. As the number of such devices in a particular network area rises, network performance worsens due to interference among participating nodes and a lack of network bandwidth [1]. Then there were worries expressed regarding the security of the Internet of Things (IoT). Communication may take occur without secrecy or authenticity due to the nature of IoT, making it subject to assaults. Traditional network security approaches, on the other hand, involve network edge firewalls and intrusion prevention or detection systems to prevent external threats. [2] but, none of the above-mentioned mechanisms won’t work directly against the IoT networks due to their advanced characteristics. New technologies such as SDN stand for software-defined networking, and it enables a centralized application known as the 'SDN Controller' to control the entire behavior of the network [2]. The controller offers a global view of the whole network, as well as rapid reactions to security threats, powerful traffic filtering, and full security policy execution. This might help SDN to decouple control operations from the forwarding layer and design network services that aren't controlled by the controller (control Plane) [3]. This means, that SDN divides the data and control planes, and then uses the network controller to make essential selections for dynamic allocation of network resources based on the network traffic. SDN is capable of efficiently adapting to changing network requirements [1]. This aspect of SDN is crucial for H-IoT applications because all these applications require wide throughput and reduced latency.

II. RESEARCH STATEMENT

This study covers the literature on Cybersecurity Threats and Mitigations in the Healthcare Sector with emphasis on the Medical Internet of Things and SDN. This also addresses how the specified technology has been advanced with the H-IoT and future advances in the field. Moreover, the most typical flaws with threats and how they can affect the broader domain will be reviewed. Most recent and emphasized attack scenarios, attack landscapes, and indicate realistic remedies will also be addressed focusing on future resolutions that will make the healthcare sector more secure will be presented.

III. REVIEW OF LITERATURE

1. Criticality of The Healthcare Sector

Warfare, pathogenic attack, and natural disasters are among the threats that the healthcare and public health sectors guard against. Because the vast majority of the corporation's facilities are privately owned and controlled, integrated information interchange between the public and private sectors is crucial to increasing the resiliency of the state's Healthcare and Public Health critical infrastructure. When a catastrophic or man-made disaster strikes, the sector, which works in all 50 states, territories, and tribal regions, plays a critical part in response and recovery across all other sectors [4]. While healthcare is normally provided and regulated at the local level, the public health sector, which focuses on population health, is handled at all levels of government: national, state, regional, municipal, tribal, and territorial. Communications, Emergency Services, Energy, Food and Agriculture, Information Technology, Transportation Systems, and Water and Wastewater Systems all rely extensively on partner sectors to ensure the continuity of operations and service delivery in the healthcare and public health sectors. [4].

2. Medical Internet of Things [MIoT]

The significance of medical IoT (IoMT) is being magnified by the synergistic expansion of artificial intelligence (AI) and the importance of medical IoT (IoMT) is being heightened by the synergistic growth of artificial intelligence (AI) and machine learning (ML). Healthcare technologies have the potential to improve, save, and enrich people's lives. Innovations vary from those that store electronic health records (EHRs) to those that oversee health and create medicine (including multifunctional gadgets and wearables, as well as technology integrated within the human body) to those that administer treatment remotely - even across nations [5]. Patients are increasingly using their mobile applications, which may now be combined with telemedicine/telehealth and integrated into the medical Internet of Things for collaborative sickness management and care coordination. As healthcare technology progress, so does its interconnection. Previously isolated, some are now joined into the hospital network. In the United States, there are presently 10-15 linked gadgets per bed. Interconnection provides several advantages, including increased efficiency, error reduction, automation, and remote monitoring [5]. These benefits are changing the way acute and chronic long-term diseases are managed. Beyond the clinical context, interconnected technologies enable health practitioners to monitor and replace implanted devices without the need for a hospital visit or invasive procedures.

In the healthcare industry, data protection has the potential to put people's lives in danger very quickly. In England and Wales, most NHS trusts provide app services as web apps with a range of backup stores, the most prevalent of which being static file stores and databases [6]. Workstations, laptop PCs, and mobile devices all have them. Test results, radiography, and real-time live patient physiological indicators will all be accessible through the internal infrastructure. Inaccessible if these specified services are taken down or effectively targeted. Medical equipment may potentially be hijacked, for example, through DDoS assaults on the Wi-Fi networks that they utilize to communicate with centralized monitoring stations. Since data is exchanged through so many computers, there is an additional risk of data theft [6]. For anyone even without literacy in healthcare infrastructure, the above example is an ideal statement to understand how important the domain is.

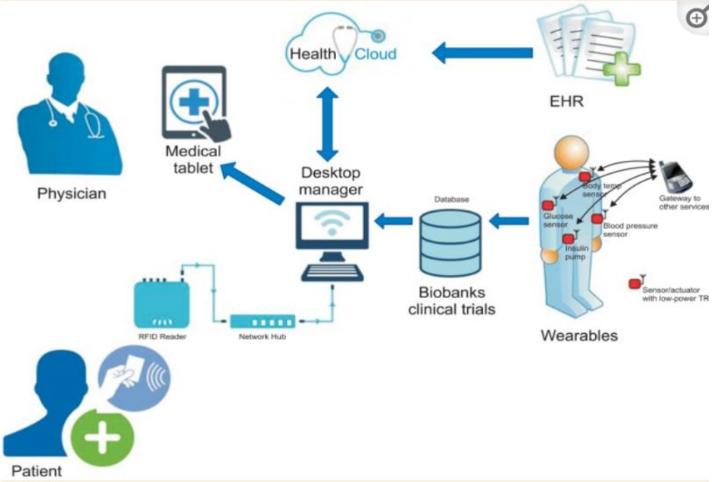


Figure 2.1

3. Assets of Medical Internet of Things

i. Sensors, Wearable devices

A standardized architecture design supports wearables, sensor systems, mobile phones, clinical applications, and healthcare station analyzers for further diagnosis and data storage. This covers hardware and software for wearable devices, sensors, smartphones, medical apps, and medical station analyzers. Wearable devices are now at the center of practically every Internet of Things concern. Because of the predicted significant rise in the population of seniors through 2020 [7], the demand for self-health monitoring and preventive medicine is increasing. Wearables have evolved greatly because of increased technology, and they are now acknowledged as trustworthy instruments for long-term health monitoring systems. These are used to monitor a wide range of environmental health monitoring indicators, as well as vital signs and fitness. Wearable healthcare equipment includes fitness trackers, smart health watches, wearable ECG monitors, wearable blood pressure monitors, and biosensors [7].

ii. Electronic Health Record (EHR) Systems

A digital record of a patient's health-related data can be generated, acquired, maintained, and viewed by permitted doctors and personnel inside a single health care organization [8]. EHRs are patient-centered, real-time records that make information instantly and safely available to authenticated parties. While an EHR system includes patients' medical and pharmacological histories, it is intended to go beyond normal clinical data acquired in a provider's office and can give a more holistic view of a patient's treatment. EHRs are a crucial component of health IT since they store a patient's medical history, diagnosis, medicines, treatment plans, vaccination dates, allergies, radiographic photos, and lab and test results. When deciding on a patient's therapy, they can also provide practitioners with access to evidence-based information. Another key advantage of an EHR is that authorized persons may access and preserve patient information in a digital platform, which can later be shared with other staff via various health care institutes [8]. EHRs are intended to exchange information with other health care professionals and organizations, such as hospitals, physicians, medical imaging facilities, pharmacies, emergency rooms, and school and workplace clinics, and thus contain information from all practitioners involved in a patient's care.

iii. MIoT Analytics Engines & Apps

IoT technology interconnects multiple devices with each other using networks, this feature has the potential to be extremely useful in the medical field. These networked devices generate a large amount of data and with the help of IoT analytics engines, doctors frequently use the generated information to forecast health trends. It also aids in determining the impact of various medications on various people. Other than that, MIoT apps can be advantageous since they aid in delivering superior healthcare solutions to patients. With the deployment of IoT devices and applications, patients are supplied with the finest healthcare warnings. The IoT apps, when paired with the experience of doctors can aid in producing vital health alerts. This function aids the patients in obtaining the most appropriate warnings based on their health.

4. Software Define System (SDN)

SDN (software-defined networking) is the isolation of controlling and forwarding operations in a network, allowing for increased automation and programmability [14]. This indicates that SDN separates the control plane and data plane. Load balancing, access control, and bandwidth distribution are examples of network operator-configured applications on the application plane. The SDN network controller has a global view of the network and can allocate resources based on changing system requirements. The network operator establishes traffic routing regulations, but the centralized network controller allows for automated network administration. To address increased network demand, network resources might be virtualized. Network function virtualization (NFV) in combination with SDN improves network performance while cutting capital and operational expenditures (CAPEX and OPEX) [1]. The network controller allows network devices and applications to communicate with one another. As the network expands, the number of network controllers included in the network may be increased to maintain network performance with increasing traffic load. SDN creates a centralized network brain that can interact with and command the rest of the network. This enables network engineers and administrators to respond quickly to changes in business demands using a centralized management interface that is separate from the network's physical hardware.

i. Architecture

There are three layers in SDN architecture.

1. Application Layer
   - Comprise all applications and services operating on the networks

2. Control Layer
   - Controller or “the brains” is a software that provides a centralized overview of the network

3. Infrastructure Layer
   - routers and switches, as well as the actual infrastructure that supports

To communicate across these layers, SDN uses northbound and southbound application program interfaces (APIs), with the northbound API interacting with the application and control layers and the southbound API communicating with the infrastructure and control layers.

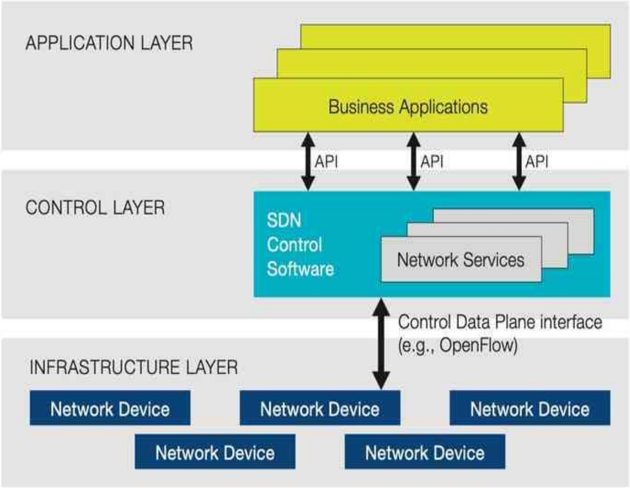


figure 4.1.1

- SDN Controller

The software that delivers a centralized view of and control over the full network is known as an SDN controller [15]. Network administrators employ the controller to oversee how traffic is handled by the underlying infrastructure's forwarding layer. The controller is also in charge of enforcing network limitations. Network administrators create policies that apply to all network nodes equally. Network policies are rules that are applied to traffic to define the amount of network access, the number of resources it is provided, and the priority it is given. With a single network image and regulations in place, network administration becomes more uniform and consistent.

- Northbound API

The apps utilize northbound APIs to interact with the control layer, telling itself of the resources that require and where they want to go. The control layer governs how programs have access to network resources and utilize intelligence to find out which path is the best in terms of latency and security for the application [15]. RESTful APIs are widely utilized in northbound APIs. Orchestration is completely automated and does not require any manual setup.

- Southbound API

The SDN controller communicates with network equipment such as routers and switches using southbound APIs. The controller tells the infrastructure which direction the application data must take. In real-time, the controller may change how the routers and switches transfer data. Devices and routing tables are no longer used to determine where data goes. Instead, the controller's intelligence makes intelligent judgments that improve data flow [15].

5. Cybersecurity Challenges in Healthcare Sector

The healthcare business has long been an intriguing target for hackers. Both the government and the private sector acknowledge this new age. With advancements in automation, interoperability, and data analytics, the risk of severe healthcare cyberattacks is increasing [12]. From high-value patient data to a low tolerance for downtime that could disrupt patient care, fraudsters continue to find ways to exploit healthcare cybersecurity standards. The healthcare business has experienced a 55 percent growth in cybersecurity risks in recent years, turning healthcare provider assaults into a $13.2 billion industry and a gold mine for hackers [10]. If healthcare providers do not take the necessary precautions to safeguard their networks, cyber threats will continue to damage the industry. IT specialists have also discovered that nations with more expensive healthcare are targeted at a higher rate, to obtain personal health information (PHI), which may be more valuable than credit card information. Malware that compromises system integrity and patient privacy, as well as distributed denial of service (DDoS) assaults that impede institutions' ability to provide patient care [11], are among the problems.

Healthcare organizations have many parallels with other businesses in terms of technology and cybersecurity. In addition to technical difficulties, needs, and limits, healthcare businesses and public health organizations confront specific cybersecurity risks in healthcare. According to the Verizon 2021 Data Breach Investigations Report, the healthcare business has experienced a significant surge in data breaches, going from 304 to 521 occurrences in the previous year [12]. Healthcare organizations have been the subject of some of the most well-known cyber-attacks in the recent decade. Community hospitals, independent physicians, and dentists may not always be able to afford to engage in costly cybersecurity measures. Nonetheless, they are prone to cyber-threats and provide thieves similar opportunities. According to the American Medical Association, approximately 57 percent of medical practices in the United States include ten or fewer doctors, with over 10% being solo practitioners [11].

6. Healthcare Data Breaches' Statistical information

The Verizon data breach report 2021 provides an in-depth look at how data breaches affect the healthcare industry. As a result, the number of breaches and accidents documented in our whole dataset has increased significantly, as evidenced by the Healthcare vertical. This organization's reported data breaches increased from 304 in the prior year's study to 521 this year [12]. However, given the HHS advice on ransomware situations, assaults in healthcare are more significant than they may be in another industry, even though the data is just at risk and not a confirmed breach. Faster operations, improved efficiency, lower costs, higher patient services, and better user experiences for internal personnel have all benefited from technology improvements in the healthcare business. Internal misuse, however, is pervasive and expanding at an alarming pace, according to the Verizon study, culminating in data breaches. Internal misappropriation appears to be the result of both planned activities and human mistakes, making the security team's task even more difficult [12].

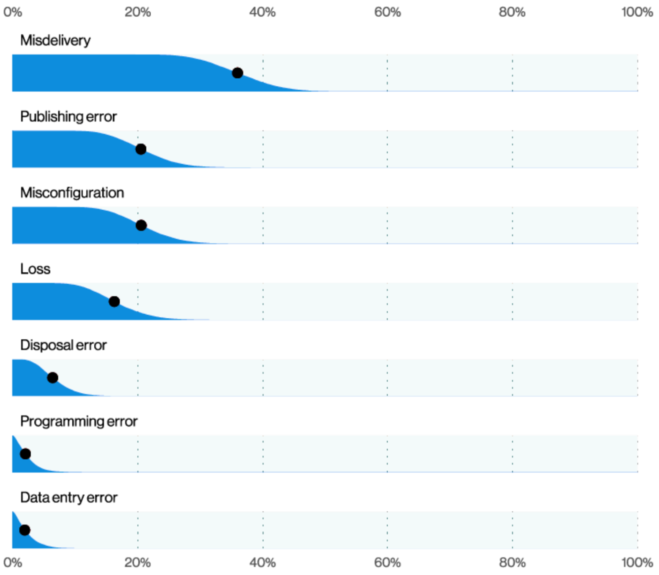
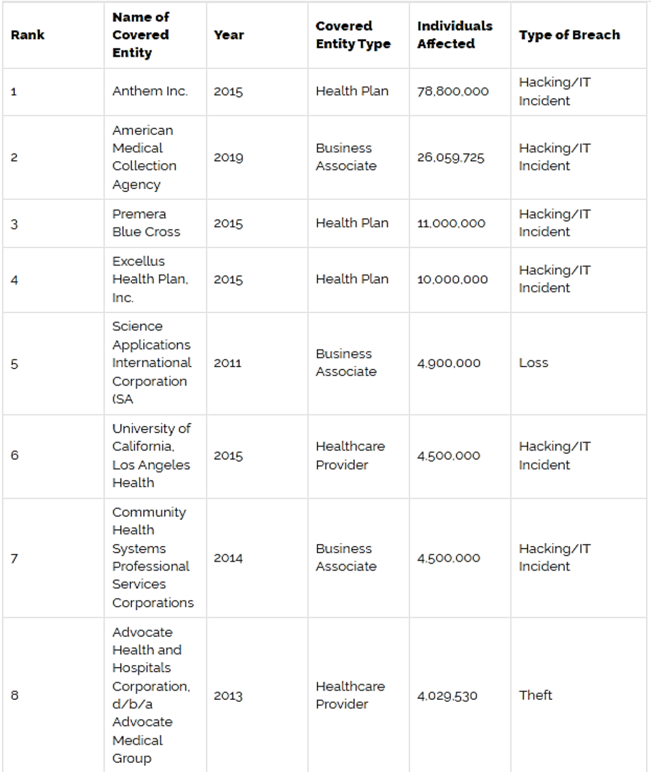


Figure 6.1

7. Healthcare Security Incidents

The volume of documents provided has been continuously growing year after year, according to the HIPAA Journal, with a significant increase in 2015. Due to the three big breaches at Premera Blue Cross, Excellus, and Anthem Inc., 2015 was the worst year in history for healthcare data breaches, with more than 113.27 million records exposed, stolen, or improperly shared [13]. The graph below depicts the significant security breaches that occurred during the previous decade..



Rank	Name of Covered Entity	Year	Covered Entity Type	Individuals Affected	Type of Breach
1	Anthem Inc.	2015	Health Plan	78,800,000	Hacking/IT Incident
2	American Medical Collection Agency	2019	Business Associate	26,059,725	Hacking/IT Incident
3	Premera Blue Cross	2015	Health Plan	11,000,000	Hacking/IT Incident
4	Excellus Health Plan, Inc.	2015	Health Plan	10,000,000	Hacking/IT Incident
5	Science Applications International Corporation (SA	2011	Business Associate	4,900,000	Loss
6	University of California, Los Angeles Health	2015	Healthcare Provider	4,500,000	Hacking/IT Incident
7	Community Health Systems Professional Services Corporations	2014	Business Associate	4,500,000	Hacking/IT Incident
8	Advocate Health and Hospitals Corporation, d/b/a Advocate Medical Group	2013	Healthcare Provider	4,029,530	Theft

Figure 7.1

8. Most Common Threat related to healthcare

The threat can be any predicament or action that could cause negatively affect organizational effectiveness (including mission, operations, appearance, or prestige), organizational resources, people, other institutions, or the Government through an information system via unauthorized access, obliteration, disclosure, alteration of data, and/or denial of service [16]. Identifying the core causes of attacks to ensure network security is highly crucial. Followings might be recognized as the common underlying reasons for healthcare cyber dangers.

- Managing budgetary constraints

In comparison to other regulated businesses, the healthcare industry spends significantly less on cybersecurity. That is, without an appropriate budget, implementing basic security measures would be more difficult, and installing budgetary gadgets may be considerably riskier.

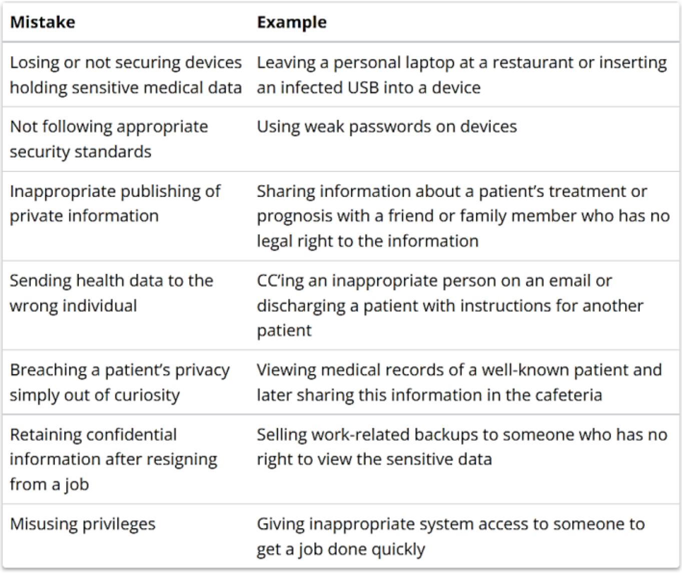
- Insider Threats

According to the 2019 Data Breach Investigation Report (DBIR), security flaws in healthcare occur more frequently than in other sectors [16], and this is one of the most difficult forms of assault to avoid. Many disgruntled or maliciously motivated employees have put healthcare organizations at risk by establishing internal access points to a hospital's network.

- Stolen or Lost assets
- Misusage of Privileges
- Attacks on Web apps

- Mistakes & Human Errors

Many healthcare security mishaps are the consequence of an avoidable human mistake. The following figure shows the common human errors and mistakes with the examples.



Mistake	Example
Losing or not securing devices holding sensitive medical data	Leaving a personal laptop at a restaurant or inserting an infected USB into a device
Not following appropriate security standards	Using weak passwords on devices
Inappropriate publishing of private information	Sharing information about a patient's treatment or prognosis with a friend or family member who has no legal right to the information
Sending health data to the wrong individual	CC'ing an inappropriate person on an email or discharging a patient with instructions for another patient
Breaching a patient's privacy simply out of curiosity	Viewing medical records of a well-known patient and later sharing this information in the cafeteria
Retaining confidential information after resigning from a job	Selling work-related backups to someone who has no right to view the sensitive data
Misusing privileges	Giving inappropriate system access to someone to get a job done quickly

Figure 8.1

- Risks that are associated with a Centralized Management system

In centralized management, a single point of failure affects the entire network [15]. Because of that one flaw of the centralized management, will break the whole SDN architecture.

- SDN Controller bottleneck

If just one instance of an SDN controller is available, a network with a substantial amount of traffic, routers, and switches may experience a bottleneck [15].

9. Current Attack landscape on MIoT and SDN

Because of a combination of inadequate cybersecurity safeguards, sensitive data storage, and a pressing need to preserve business continuity at all costs - an inevitability exacerbated by the pandemic [16], the healthcare industry is a popular target for hackers. The following cyber-threats represent the greatest danger to the security of patient information and healthcare data and the graphic below depicts the cyberattack lifestyle.

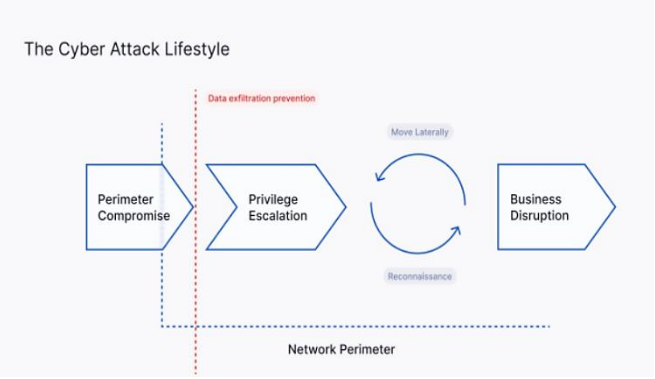


figure 9.1

i. Social Engineering Attack

Pretexting & Phishing : Attacks that initiate social engineering strategies to abuse healthcare organizations' confidence in their staff and patients are common in the healthcare industry [17]. A classic phishing campaign, for example, entails healthcare professionals receiving emails purporting to be from healthcare organizations and being instructed to click on links or open attachments. This action may result in the disclosure of sensitive healthcare data as well as healthcare cyberattacks..

ii. Data Breaches

When compared to other businesses, the healthcare industry experiences a disproportionately high number of data breaches. In 2020, the average number of data breaches in the healthcare sector per day was 1.76 [16]. While most businesses in other sectors protect essential assets and sensitive information from unauthorized access, many health institutions fail to implement adequate security measures to protect their healthcare information, records, and crucial infrastructures. Such cybersecurity gaps allow cyber attackers to get access, putting the security of medical care data at risk. Major data breaches are likely since the threat environment allows for indirect access to sensitive data such as social security numbers, credit card details, and even medical device intellectual property. Instead of a comprehensive cybersecurity overhaul, such overlooked vulnerabilities might be detected with an attack surface monitoring system, which would need to be supported by healthcare security expenditures to be sustained [16].

iii. Software Attack

Software assaults are defined as poorly built applications that have a malicious effect on healthcare equipment, computers, or servers. In a hospital setting, integrated and tailored software is increasingly being deployed, and patient treatment and tracking are unquestionably improving. However, a sufficient level of safety precaution is not used to verify the operation and validity of medical apps. Keeping these principles in mind, healthcare systems are subject to a variety of software and app-related assaults, such as,

Malware : Malware is any program or code that has been maliciously produced. A malware-infected healthcare system may cause the equipment to slow down or shut down. Due to unpartitioned networks, dependence on legacy systems, lack of compliance controls, uncontrolled IoT devices, and vulnerable medical management apps [19], may vulnerable healthcare systems to all sorts of malware.

A group of academics at Ben-Gurion University's cybersecurity lab recently discovered a new type of malware capable of changing the findings of medical tests. The malicious software, which may infect CAT and MRI scanners, can insert bogus malignant tumors into medical reports, misleading doctors and potentially causing significant difficulties in medical facilities. [19].

- LokiBot Malware - Lokibot is a data thief; whose binary's primary goal is to capture system and application credentials, as well as user information, and then deliver it to the attacker.

- Fareit Malware - This malware is mostly used to capture user and FTP credentials and passwords, download other payloads, and connect infected systems to a botnet.

- Remcos-RAT - This is a legal program designed for administrators to utilize for remote access and maintenance. that has lately been utilized in attempted hacks, where it was disguised as part of the payload using COVID-related phishing themes.

- Agent Tesla - Agent Tesla's proper implementation gives attackers full access to a computer or network, allowing them to gather credentials, sensitive information, keystrokes, screen, and video activity, and form data.

- Formbook Malware - Formbook, usually referred to as "form grabber" malware, is a type of malware that grabs information. The malware is installed on victims' Computers when they visit fraudulent web pages or domains.

Ransomware : Ransomware limits access to a computer or server until a ransom payment is paid. Because hospitals rely on information technology systems to deliver crucial patient care, ransomware may be devastating if important care procedures are affected [18]. WannaCry is the ransomware that disrupted the UK's National Health Services (NHS) in 2017, costing them £92 million [19].

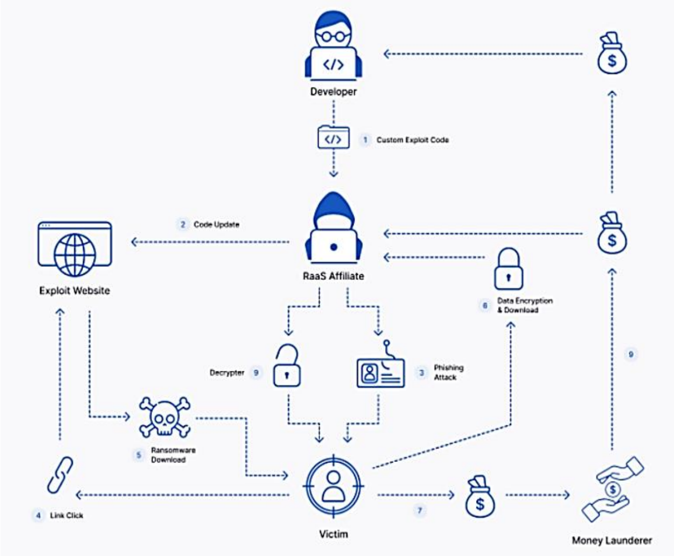


Figure 9.2

iv. Denial of service [DOS] and DDOS attack

A DoS attack floods the network with massive amounts of traffic all at once, preventing legitimate users from gaining access unless they pay for priority service. A healthcare DDoS attack is a more sophisticated version of a DoS attack in which hackers use botnets to redirect enormous quantities of online traffic at healthcare institutions.

10. Countermeasures for current threats

i. HIPAA Compliance

The Health Insurance Portability and Accountability Act of 1996, often known as the HIPAA Act, is abbreviated as HIPAA. It is a privacy statute in the United States that protects medical information like as health records and allows patients and healthcare practitioners to interact securely [20]. On August 21, 1996, the 104th US Congress adopted President Bill Clinton signed the HIPAA Act. The HIPAA Act is also known as the Kennedy-Kassebaum Bill since it was originally introduced in Congress as the Kennedy-Kassebaum Bill. Both Democratic Senator Edward Kennedy and Republican Senator Nancy Kassebaum were vocal supporters of the bill. HIPAA has two primary goals, as stated in the act's Titles I and II [20].

- Title I – Health Care Access, Portability, and Renewability

Title, I cover employers' and their families' health care coverage when they alter or terminate their employment.

- Title II – Preventing Health-Care Fraud and Abuse; Administrative Simplicity; and Medical Liability Reform

Title II requires insurers, healthcare providers, and employers to create national IDs, as well as standardized standards for electronic healthcare transactions. The Act also protects health data and privacy. The HIPAA Administrative Simplification criteria require the Department of Health and Human Services to adopt national standards for health identities, protection, electronic health care transactions, and code sets (DHHS). Medical Liability Reform suggests that healthcare practitioners who violate the law suffer legal consequences [22].

ii. Privacy Policies

The purpose of the Privacy Rule is to establish fundamental Federal rules for preserving the privacy of publicly identifiable health information. Covered firms that must comply with the Rule include health insurers, health insurance clearinghouses, and some healthcare providers [21]. Except as allowed or required by the Privacy Rule, covered entities are not permitted to use or report PHI.

Individuals may be granted certain rights under the Rule, including the opportunity to see and change their health information and provide proof of when and how their PHI was shared with others for certain purposes. Furthermore, covered businesses are subject to administrative procedures under the Rule. Covered entities that breach the Privacy Rule [21] may face civil monetary penalties, criminal monetary fines, and/or imprisonment.

IV. FUTURE RESEARCH

As healthcare IoT and SDN technology evolves, new risks and vulnerabilities emerge. To be more specific, the resilience of critical healthcare technology degrades as new technologies are adopted for the sake of convenience and cost savings. As a result, it is necessary to develop innovative defense mechanisms to supplement or augment existing critical healthcare systems. A viable method is to create security systems that function from a full scope of critical infrastructure and integrate structured reactions to interruptions using behavioral analysis. Many new studies and deployments are testing and advancing fast to protect healthcare systems, MIoT devices, and networks, particularly in the healthcare business.

V. CONCLUSION

Widespread coverage and fast speeds are becoming increasingly necessary as the population and workload expand, necessitating new and more intense services. Today's community would very probably be unable to function efficiently if major components of the system were corrupted or lost. It's an excellent time to try to increase your network of healthcare connections. The increased connectivity of physical and digital systems with linked devices, equipment, and systems presents new security issues for these businesses, particularly in terms of accessibility. A key defensive action that institutions should take in response to these new healthcare technologies is to mitigate risks such as breach of security, disclosure of personal data, or harm to property, while also safeguarding patients, people, and the surrounding community. A great deal of time and effort has been spent here studying current industrial concerns, and new technological breakthroughs have been included in this subject. Furthermore, the research looked at the many sorts of dangers and how the best approaches to tackle these risks were eliminated. Because medical apps fulfill critical functions, it is critical that the community deal with them aggressively and pro-actively. The types of vulnerabilities utilized by attackers to breach healthcare systems during the most recent event have been investigated to determine how they were exploited. The discovery of data and resources was utilized to create a picture of a probable assault situation. Numerous concepts are helpful to the proposed area, but only a few have been picked for investigation, and many of the ways for mitigation and possible future developments have already been chosen. As a result, it is believed that readers who read the article will be able to follow what has been mentioned in prior publications or presentations on the fundamentals of the review.

VI. ACKNOWLEDGMENT

The authors are grateful to Mr. Kanishka Yapa, our lecturer in charge of the Applied Information Insurance module, who has aided and motivation since the beginning of this project. I'd also like to thank all my colleagues who contributed to the success of this research. Finally, I'd like to express my heartfelt gratitude to everyone who contributed resources and ideas to help me complete this project on time.

VII. REFERENCES

[1] Rinki Sharma "Software Defined Networking for Healthcare -Internet of Things Throat GPS: Global Positioning System GSM: Global System for Mobile communication H-IoT: Healthcare Internet of Things ID: Identifier IEEE: Institute of Electrical and Electronics Engineers IoT: Internet of Things IP: Internet Protocol IPv6: Internet Protocol version 6 IrDA: Infrared Data Association" researchgate.net [Online]. Available: https://www.researchgate.net/publication/355734834_Software_Defined_Networking_for_Healthcare-Internet_of_Things_Throat_GPS_Global_Positioning_System_GSM_Global_System_for_Mobile_communication_HIoT_Healthcare_Internet_of_Things_ID_Identifier_IEEE_In (accessed March 24 2022)

[2] Abdullah Al Hayajneh, Md Zakirul Alam Bhuiyan and Ian McAndrew "Improving Internet of Things (IOT) Security with Software Defined Networking (SDN)" researchgate.net [Online]. Available: https://www.researchgate.net/publication/339121533_Improving_Internet_of_Things_IoT_Security_with_Software-Defined_Networking_SDN

[3] Sahrish Khan Tayyaba, Naila Sher Afzal Khan, Wajeeha Naeem, Munam Ali Shah, Yousra Asim and Muhammad Kamran "Software-Defined Networks (SDNs) and Internet of Things (IoTs): A Qualitative Prediction for 2020" thesai.org [Online]. Available: https://thesai.org/Downloads/Volume7No11/Paper_51-Software_Defined_Networks_SDNs.pdf (accessed March 24, 2022) "

[4] "Healthcare And Public Health Sector" cisa.gov [online]. Available: https://www.cisa.gov/healthcare-and-public-health-sector (accessed March 24, 2022)

[5] Lynne Conventry "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward" academia.edu [online]. Available: https://www.academia.edu/48662174/Cybersecurity_in_healthcare_A_narrative_review_of_trends_threats_and_ways_forward (accessed March 24, 2022)

[6] S. Walker-Roberts, M. Hammoudeh, and A. Dehghantanha, "A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure" ieeexplore.ieee.org [online]. Available: https://ieeexplore.ieee.org/document/8320362 (accessed March 24, 2022)

[7] Mostafa Haghi, Kerstin Thurow and Regina Stoll "Wearable Devices in Medical Internet of Things: Scientific Research and Commercially Available Devices" pubmed.ncbi.nlm.nih.gov [online]. Available: https://pubmed.ncbi.nlm.nih.gov/28261526/ (Accessed March 25, 2022)

[8] "Electronic Health Record Systems" hhs.gov [online]. Available: https://www.hhs.gov/sites/default/files/electronic-health-record-systems.pdf (accessed March 25, 2022)

[9] Djamel Eddine Kouicem, Abdelmadjid Bouabdallah, and Hicham Lakhlef "Internet of things security: A top-down survey" sciencedirect.com [online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1389128618301208 (accessed March 25, 2022)

[10] "The Top 6 Cybersecurity Challenges in the Healthcare Industry" securityscorecard.com [online]. Available: https://securityscorecard.com/blog/top-cybersecurity-challenges-in-healthcare-industry (accessed March 25, 2022)

[11] "Cybersecurity in Healthcare: Major Threats and Challenges" delveinsight.com [online]. Available: https://www.delveinsight.com/blog/cybersecurity-in-healthcare-industry (accessed March 25, 2022)

[12] "Cybersecurity Challenges in Health Care Industry" iquasarcyber.com [online]. Available: https://iquasarcyber.com/cybersecurity-challenges-in-healthcare-industry/ (accessed March 25, 2022)

[13] "The Healthcare Data Breach Statistics" hipaajournal.com [Online]. Available: https://www.hipaajournal.com/healthcare-data-breach-statistics/ (accessed March 28, 2022)

[14] Himanshu Arora and Tarun Thakur "Software Defined Networking (SDN) explained for beginners" howtoforge.com [Online]. Available: https://www.howtoforge.com/tutorial/software-defined-networking-sdn-explained-for-beginners/ (accessed March 28, 2022)

[15] "What Is Software Defined Networking (SDN)? Definition" sdxcentral.com [Online]. Available: https://www.sdxcentral.com/networking/sdn/definitions/what-the-definition-of-software-defined-networking-sdn/ (accessed March 28, 2022)

[16] Edward Kost "Biggest Cyber Threats in Healthcare" upguard.com [Online]. Available: https://www.upguard.com/blog/biggest-cyber-threats-in-healthcare (accessed March 28, 2022)

[17] Harman Singh "Healthcare Cybersecurity: Threats and Mitigation" infosecurity-magazine.com [Online]. Available: https://www.infosecurity-magazine.com/blogs/healthcare-cybersecurity-threats (accessed March 28, 2022)

[18] "5 Ways Attackers Are Targeting the Healthcare Industry" tripwire.com [online]. Available: https://www.tripwire.com/state-of-security/healthcare/attackers-targeting-healthcare-industry/ (assessed by March 28, 2022)

[19] "Sophisticated threats plague ailing healthcare industry" blog.malwarebytes.com [online]. Available: https://blog.malwarebytes.com/cybercrime/2019/04/sophisticated-threats-plague-ailing-healthcare-industry/ (assessed by March 28, 2022)

[20] "HIPAA 101: What does HIPAA stand for? - HIPAA HQ." hipaahq.com [online]. Available: https://www.hipaahq.com/hipaa-101-what-does-hipaa-stand-for (assessed by March 28, 2022)

[21] "HIPAA-Compliant Privacy Policy Language for e-Health Applications" iapp.org [online]. Available: https://iapp.org/resources/article/hipaa-compliant-privacy-policy-language-for-e-health-applications/ (assessed by March 28, 2022)

VIII. AUTHOR PROFILE

Dilshan K.N
3rd year 1st semester Undergraduate in
BSc (Hons) in Information Technology specializing in Cybersecurity.
Sri Lanka Institute of Information Technology,
Malabe, Sri Lanka