Cyber Security threats and mitigations in the Healthcare Sector with emphasis on medical Internet of Things and SDN.

O. D Abeywickrama
Faculty of Computing (Speaclizing in Cyber Security)
Sri Lanka Institute of Information Technology (SLIIT)
Malabe, Sri lanka
It20153540@my.sliit.lk

***Abstract*—Due to the obvious importance of medical information in human health, an increase in cyber-attacks on the medical profession has resulted in huge losses in the health-care industry. The Internet of Things (IoT) has become an essential component of industry operations in recent years. IoT applications have increased significantly in healthcare, agriculture, supply chain, smart energy, building and industrial automation, and connected automobiles. This chapter focuses on the healthcare business. The chapter discusses the advantages, disadvantages, and potential solutions of using Software Defined Networks (SDN) in Healthcare-Internet of Things, as well as the applications and challenges of implementing IoT in the healthcare industry (IoT).**

Keywords — Healthcare sector, Cyber security threats, Mitigations, Security, IoT, SDN.

I. INTRODUCTION

In the last several years, the healthcare industry has experienced an increase in cybersecurity incidents. Malicious hackers have stolen millions of documents from the computers of major corporations including Anthem, Premera Blue Cross, and Excellus. In the healthcare area, however, health data records aren't the primary goal.

Internet-enabled insulin pumps, pacemakers, MRI machines, and other medical gadgets have all emerged as a result of the Internet of Things' (IoT) revolution. In the medical industry, there are currently more worries about personal data breaches. According to Boan News , the banking and healthcare industries are the most concerned about data breaches, accounting for 49.45 percent and 28.41 percent of breaches, respectively [1].

Finance is a typical target for hackers since the records are full of financial transactions. Healthcare security measures receive less attention than financial security measures, despite the fact that medical data is far more valuable and sensitive. Each connection might alternatively be made up of many networks. For example, obtaining a patient record from a connected IoT enabled medical imaging device necessitates maximum bandwidth from the appropriate hospital's network, as well as agility and flexibility. Traditional networks necessitate innovation as well as the ability to deal with the aforementioned difficulties [3].

One of the most appealing IoT application areas is medical care and health care. Many medical applications, such as remote health monitoring, fitness programs, chronic illnesses, and senior care, have the potential to be enabled by the Internet of Things. Another significant potential use is adherence to treatment and medication at home and by healthcare providers. As a result, different medical equipment, sensors, and diagnostic and imaging devices can be seen as smart devices or objects that are an essential component of the Internet of Things.

Healthcare services offered by the Internet of Things are intended to save costs, increase the quality of life, and improve the user experience. Remote provisioning through the Internet of Things, according to healthcare providers, has the potential to minimize device downtime.

SDN (software-defined networking) is a novel way to updating existing networks. The separation of the infrastructure plane from the controlling layer is crucial for solving the problems of IoT enabled devices. The SDN Architecture oversees the whole network and has global visibility [2].

SDN not only fixes common network issues, but it also adds a slew of new capabilities to let IoT-enabled networks reach their full potential. In the healthcare industry, clinical trial networks, which are made up of many subnetworks, are becoming more widespread. SDN involves acting as a backbone to support and execute the functionality due to the rising number of patients admitted, hospitals accessing these connections, diagnostic supplies, and many other elements.

As healthcare progresses toward later part IoT-enabled devices, such devices communicate with one another across a network. There are certain advantages to this, but there are also some negatives. A network that can handle the challenges of IoT-enabled networks is necessary. Security is one of the challenges since crucial information regarding each patient's health is one of the worries.

Shodan, a search engine for the Internet of Things, is one tool that might help find potentially susceptible Internet-

enabled medical equipment. Shodan's billion-record database is accessible via a web interface and/or API. Figure 1 depicts how a user may find and utilize a medical equipment produced by Omron Corporation, a leading medical device provider.

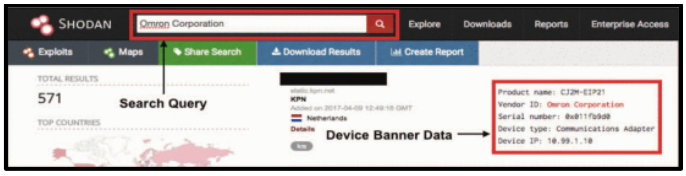


Figure 1 : Shodan results for Omron corporation search.

The purpose of this study is to uncover vulnerabilities in the medical devices that might be identified in we API's which is used to gather thousands of devices from leading medical device manufacturers, and nessus vulnerability assessment tool can also be used to investigate vulnerabilities of the devices

The rest of the paper is organized as conducting a research on medical equipment and vulnerability assesments. assessments. In the second paragraph, explain what a research testbed is. Then, describe the most important findings and outcomes. Finally, make a conclusion and suggest ideas for more research.

Research statement.

Due to the importance of medical information in human health, a rising number of cyber-attacks in the medical profession have resulted in significant losses in the health care business. This article begins with a quick review of the essential backdrop of the dataflow in the medical sector and then analyzes the vulnerabilities at each stage of the dataflow to offer a full survey regarding probable cyber-attacks and remedies for these assaults. Then, based on the medical system's vulnerabilities, a classification of cyber-attacks is offered.

In addition, the study offers findings from prior research aimed at resolving these cyber-attacks, as well as the strengths and limits of each approach. More crucially, the research explores potential cybersecurity designs for the medical domain from the current literature for data storage assurance. Previous countermeasures and designs that are still lacking in terms of resource depletion, attack reduction, applicability, and other factors are addressed. Finally, the study addresses and suggests options for future work in the medical profession to reduce cyber-attacks and ensure human health [4].

Existing network design fails to apply high-level network rules and manual command-line interfaces, creating a barrier in IoT enabled healthcare networks; at this point, SDN comes into play. With the assistance of SDN not only the management of the full network has become easier, but it also removes the manual command-line interface as well. You can control the flow of traffic from a specified source to a specified destination with only a few clicks. This research aims to demonstrate the importance of SDN in IoT healthcare applications. Various benefits, difficulties, and active research paths are discussed, as well as the entire architecture of both technologies.

II. LITERATURE REVIEW.

The difficulty of gathering, aggregating, and interpreting network data from diverse IoT devices has been examined. This source data can be vast and in any format, such as audio, video, or text. The authors presented a centralized and adaptable system architecture for real-time transmission of enormous volumes of data that can offer security, privacy, and other security requirements for a range of linked healthcare applications.

The chance of security breaches are rising when looking at the direct proportion to the "degree of connection". Further the medical equipment with interent connection has also increased significantly which has affected the quality of the service is a positive manner. But with these advantages comes the attackers who try to gain sensitive information in order to get money or for a personal grudge or to steal data

Many medication delivery systems such as the neurostimulators are very vulnerable for cyber attacks [3],[5] . In order to address the rising concern about the cyber threats in medical threats Food and drug Administration has set cyber security standards for 3 medical device classes(table 1) before these goods are released in to the market

Medical Device Class	Attributes	Example Devices
Class I	Common, low risk, low complexity	Lancet, Dental Floss
Class II	More complex, greater risk to patient, partially implanted	Syringe, Insulin Pump, BGM
Class III	Fully implanted, greater risk, regulate body functions	Artificial Pancreas, CGM, Replacement Heart Valves

Table 1 : Medical device classes.

Concerns concerning cybersecurity are frequently focused on class II and III devices. For example, Jay Radcliffe utilized the serial number to hack into an insulin pump, a Class II piece of equipment, and was able to send commands to the device or disable it. This might be disastrous for diabetics who rely on properly functioning insulin pumps. As an example, analyzing the vulnerabilities of other connected medical equipment to minimize potentially serious assaults is motivating.

In, there is a discussion on the use of IoT, its origins, and benefits. They also show the intricacies of the design and other component requirements. The authors offered an architecture for IoT-health care, as well as further research objectives and obstacles.

This investigation the issues and numerous concerns associated with the conventional Healthcare Monitoring System's security and privacy (HMS). They also suggested architecture as a resource. This architecture could be used to manage IoT-powered healthcare monitoring systems. It safeguards not only the security and privacy of the different

services available, but also their dependability. Several policies and services are geared for the elderly and ill.

Malasri and Wang presented an overview of healthcare implanted devices as well as certain implantable device dangers (eavesdropping and spoofing). Ida et al. talked about a rigorous examination of IoT for eHealth. The research also looked at security challenges in IoT healthcare. McMahon et al. went into great detail on IoT-enabled medical equipment. The survey, on the other hand, was restricted to identifying vulnerabilities in compromised medical devices. Masdari and Ahmadzadeh provided yet another good study of the telecare medical system's authentication taxonomy (TMS). TMS authentication approaches are also compared, as are TMS limits and advantages [6], [7].

The study done here provides a overview on the different states of IOT in different areas. The eight research directions that have been discussed is by increasing the use of sensors, communication etc.. and extract knowledge from a large amount of data [4], massively scaling, dependencies and architecture and many more are in the loop. Purpose of this study is to recommend a technological combination that incorporates SDN and IOT

Current accomplishments in various areas, such as wireless and optical domains, are highlighted in order to integrate the technologies, as are difficulties related to both technologies from the standpoints of security and scalability. SDN technology is not only gaining traction in business and academia, but it is also the most successful technology in the technological sector for lowering network traffic using a specific protocol.

McDermott et al. carried out a survey to determine the risk classifications for protecting Electronic Health Record (HER) data. This paper describes the application of IoT in healthcare. The proposed architecture focuses on protecting healthcare data from network attacks by employing a specific algorithm and protocol. In terms of security, IoT-restricted devices in the healthcare business are still in their infancy. All of the aforementioned difficulties have been addressed by this proposed solution, which is a safe, trustworthy, and certified method. Graphs are used in this study to evaluate network connectivity [8].

SDN addresses the difficulties of efficiency, scalability, manageability, and cost-effectiveness in IoT from a variety of perspectives. The challenges of edge, access, and core networking have also been considered. Many networking solutions that either assist the network with SDN or are beneficial in resolving the WSN issue have also been offered. The challenges of IoT and data center networks have also been explored, as well as how SDN might help solve them.

Due to the involvement of the IOT devices the medical care has grown by a significant amount and in popularity throughout the world in the last decade or so because of its significant reliance on the IT field. MCIS cyber security plays critical role in providing the trustworthy, secure and successful medical care. Cyber Security threats are one of the main threats that the healthcare sector face in a day to day basis

New offensive patterns affecting growing technologies such as cloud computing, social media, critical infrastructure, and smartphone technology were investigated. With the advent of cutting-edge medical technology, there is a major danger of medical technology vulnerabilities and attacks.

The study, on the other hand, was confined to discovering weaknesses in hacked medical devices. Another important evaluation is the Telecare Medical System Taxonomy (TMS). TMS authentication approaches are also compared, as are TMS limitations and advantages. A case study on the hazards of healthcare IoT using just the Markov model. However, due to the limits of the Markov model, only a few problems were found. Presents a promising review of the medical service area [9].

McDermott et al. [10] conducted a survey to determine probable danger classifications for HER data protection. Portable gadgets, physical threats, technological dangers, insider usage, and administrative dangers were all classified into five categories.

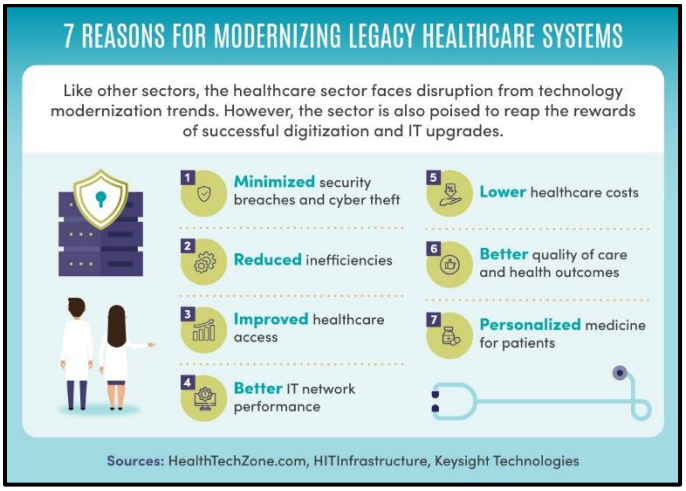


Figure 2 : Healthcare Cyber Attacks.

Fernández-Alemán et al. [11] provided the findings of a comprehensive evaluation of the literature on EHR security and privacy. The review also suggested that EHR security and privacy standards be created, and that guidelines be given.

Software development and also security, physical and logical further the business community, non technological factors are main things included in the article. Further when looking at the stats the physical security is required in more attention to detail than other because physical attacks will result in breaches which put the patient at risk

This section mentioned cybersecurity breaches such as ransomware attacks on hospitals and health information theft. In addition, deliberate assaults against well-known medical devices were conducted out. Following extensive investigation, it was discovered that all of the available surveys are incredibly essential [5]. These surveys, on the other hand, either focus on the security and privacy of implanted medical devices from an

IoT standpoint or employ specific models and case studies to authenticate the devices. The cutting-edge survey, on the other hand, evaluates the flow of information in the medical domain as well as the fundamental cybersecurity flaws in the medical domain, with a focus on data storage and IoT connection.

Such wireless connections put the gadget at danger of security breaches, raising worries about patient safety and privacy [2]. Investigators have discovered that these devices, as well as their wireless connections, are vulnerable to cyber-attacks, jeopardizing patient safety, security, and privacy.

Researchers have shown many forms of attacks on medical equipment, including privacy leaks by eavesdropping, safety and integrity flaws via message manipulation, and availability difficulties via battery draining assaults [4]. A number of mitigations have been proposed for these attacks. The resource limits on medical devices for applying security measures are a major consideration when building mitigations for them.

The most significant consideration for implantable medical devices (IMDs) is battery life. Non-rechargeable batteries are used in most electronics, and they must be changed every few years. Adding cryptographic security to communications is extremely difficult since any communication or function that affects battery life has a significant performance effect [9]. The device platform does not enable high-end encryption for communications protection, even for non-implantable devices. As a result, in recent years, lightweight cryptography for these low-end devices has been a hot research area .

Though this would let patients to move around and be monitored at all times, it will also put patients' safety, security, and privacy at risk. For further acceptance of these devices and their expanded communication functions, it will be critical to address these cyber dangers. Present an architecture for IoTs that improves their safety, security, and privacy while allowing for more mobility and monitoring in this section. For better patient safety, security, and privacy, the framework employs lightweight encryption and attribute-based permission to give fine-grained access control to device data and functionality [9].

People usually tend to use the internet to figure out different pieces of technology which are connected to different types of treatments and messages so that they can look into their health schedules. Also internet is used tin order to get different instructions on operation of different products which are linked to the therapy, also messages on the issues regarding the health and the clinic timetable. Therefore the Cyber criminals use the these chances in order to lure the people and launch different types of attacks in order to gain access to do various work. And cyber attacks have grown considerably due to the current pandemic [12]
.

Jang-Jaccard and Nepal discovered weaknesses in today's software, hardware, and network layers. Cloud computing, social media, critical infrastructure, and smartphone Different types of cyber crime such as scams make sure that they earn a considerable amount of money by making a small danger to the victim unless a proper opening is met by the scammers. Further the government and the private organizations gives aids such as financial support to individuals. People are willing to work for organizations so that they may spend more time socializing with others in their network.

These weaknesses that different organizations have are being used by the attackers in order to send mails which consists of phishing attacks to hospitals which looks into the pandemic, tax authorities and other government organizations. Wu et al Implantable medical devices are checked by multiple examinations thoroughly In order to prevent types of unwanted access and control. Studies with the concerns of the healthcare industry was carried out by Kruse et al and this was reported by Jalali et al[13].

The world economic Forum stated that the cyber-attackers are increasing becoming more and more prevalent day by day which was simply a result of illegal activities such as phishing and other types. Mainly these types of attacks takes place form emails rather than internet sources which we usually visit in a day to day basis because it is way easier to trick people into such things with an email because a person’s one of the main way of getting OTP’S and other password resets are through the mail which in turn will make a person to share their information without double checking [14]. since people are anticipated to contact the necessary parties in the work environment, therefore these scammers may take the advantage of this by making attractive emails and collecting all the job related information before carrying out a proper attack

Cybercriminals are well-versed in routes. In the software, hardware and network layers have many types of weaknesses today and some were identified by Jang-Jaccard and Nepal. New attack patterns for developing technologies such as cloud computing, social media, technologies such as smart phone technology were the go to[15].

The sender must check that the message received is valid while sending an email. When sending an email, the sender must be certain that the Received message is originally from the sender and not from a intruder because the cyber criminals are able to act like a different individual and make the receiver click on malicious sites. Vulnerabilities and other weaknesses in home employer security systems let other parties to get access to information and launch attacks. A conundrum has developed as a result of the ubiquitous isolation. Finding technical solutions has become increasingly difficult, placing the sector at danger of situations such as remote employment [16].

Information collecting attacks, database assaults, website attacks, and operation device attacks can all jeopardize cyber security. Hackers can also use cybersecurity for nefarious purposes such as forgery, data tampering, data breach, and so on. Hackers can also exploit cybersecurity for evil goals like forgeries, data alteration, data breach, and so on [17].

As a result, patient privacy is significantly jeopardized, which has a detrimental influence on treatment and medication procedures and may jeopardize the patient's health. By the security update the MS17-010 was impacted by

a attack which was a information gathering also was faced by some OpenSSH vulnerabilities. Through this security update the vulnerability which was formed gives the attacker to get the full control of the device. This subject has been approached in a variety of ways [18]. To begin, the API sequence of the ransomware can be used. Second, an alternate method may be found using the decoupled architecture and usable security.

IV. THE ARCHITECTURE OF THE NETWORK WITH SDN.

Because there are several networks with diverse networks, IoT is currently expanding into the modern era. These networks are related. Massive networks are also prevalent in IoT in healthcare. These networks are made up of a variety of hospital and other clinical trial networks. Because traditional network design couldn't manage the breadth of IoT advances, it became necessary to activate the SDN-based network with IoT.

Figure 2 depicts the proposed SDN-based IoT Healthcare Network architecture. As can be seen this network has been built by a distinct number of networks which are connected among one another in different hospitals. Several hospitals are continuing to participate in network activities to transfer data, clinical reports, and patient data across a wide range of IoT devices.

A data center houses all relevant data. The networking used in the data center consist of 3 levels of architecture. The internet protocol, which contains physical configuration, networking devices, and other network locations, is the first layer (switches, routers). The primary and control layer, which is a more centralized SDN controller, is the second and higher layer. This SDN controller supervises overall network operation and has a global view of the network [19].

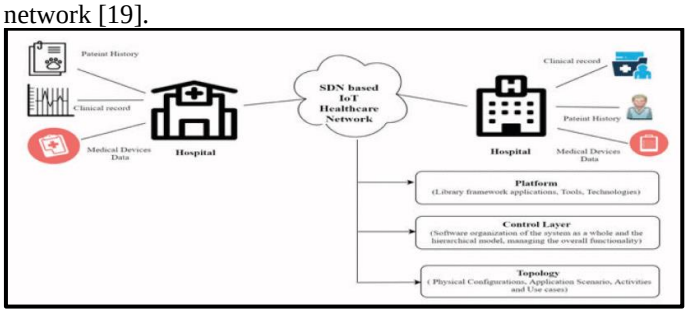


Figure 3 : The proposed architecture of SDN based IoT healthcare Network.

III. CYBER SECURITY ISSUES IN HEALTHCARE.

Healthcare sector has been subjected to a huge number of cyber attacks which makes it more vulnerable than the other industries which are present. Hackers infiltrate applications for a number of reasons. A large percentage of attackers want credentials in order to demand a ransom, while some seek credentials in order to bribe high-profile people to reveal sensitive information to the public [20]. Hospitals have already been heavily targeted as a result of these difficulties, owing to the increased use of technologies such as telehealth and electronic health records.

Common threats.

Phishing, Business email compromise, ransomware and DDoS were the threats that were mostly used in the healthcare sector for different types of motives in the healthcare sector during the pandemic; these threats were deployed in many assaults. Only a few clicks were necessary to breach the target, meaning that sending more emails boosted the success rate. Stealth was heavily used in sensitive places such as fiancees, banks, and other well-known enterprises. In order to capture the victims the attackers are using more sophisticated strategies (encrypting websites with HTTP encryption technologies) is one such way. SSL was deployed on more than 75% of phishing sites, worsening the issue. Phone apps for webmail and software as a service (SaaS) are common phishing targets [9]. Malicious software includes worms and Trojan horses.

Even during Coronavirus epidemic, attackers and APT organizations sent malware to susceptible people and networks via emails and ad sites. Seventy percent of the infection was determined to have entered the system via email. Malicious software with particular characteristics, like as ransomware, will have a significant influence on the business of the epidemic [16]. Because it is simple to deploy and has a huge impact on the target, distributed denial of service is tough to utilize. DDoS assaults, unlike regular DoS attacks, employ several attack sources and hosts to create a threat against many targets, multiplying the threat and complicating security.

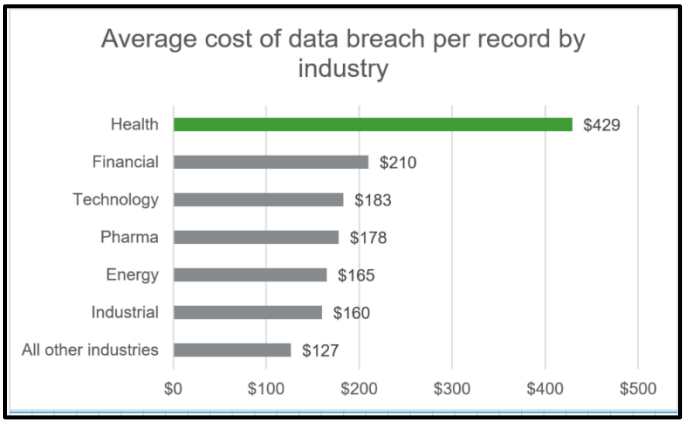


Figure 4 : Average cost of data breach per record by industry.

A. Departments impacted by the cyber actors.

1. **Information Technology Department**.

Because hospitals' IT divisions contain a wide variety of data, they are one of the most often targeted departments. As it department hasn't kept up with the trends, cyber thieves are hunting for holes, such as obsolete or susceptible systems, to launch attacks. Recent cyber-attacks have demonstrated the industry's vulnerability to cyber-security flaws.

It is also necessary to know the budget limit an healthcare organization can bare in order to defend their IT assets [21]. But many hospitals are still using old systems such as windows 7 and windows xp versions because it is easy for the hospital but it makes these hospitals more and more vulnerable than ever

Crypto locker assaults on healthcare facilities are prevalent, according to Europol. Presently in order to keep up with the current technolpgy and the security measures which are being implemented in the world everything should be digitalized and IOT devices should be connected in order for data collection, storing processing and other activities

2. Financial Department

This one has cost millions of dollars to disrupt global institutions and networks. In this healthcare industry the harmful software's (ransomware, phishing) is mainly targeted at the finance department. When looking at the loss of money in 2020 only there was a loss of about 21 billion dollars. South Africa, for example, is taking every precaution to protect its financial assets.

Now because of digital banking the customers are using their smartphones in order to do the transactions and because of the different security issues the phones have the hackers are now more accessible to information than ever. If firewall protection and other features such as internal access controls are not well understood, but if implemented, banking sector security would improve. Updates to antivirus software on PCs may make a difference in terms of security.

Financial organization workers mainly deal with sensitive data and faces a lot of security challenges because the operations are in environments which are mainly targeted by different types of hackers. Further social engineering Is one of the main attacks which should be looked at and be careful of without getting caught in them

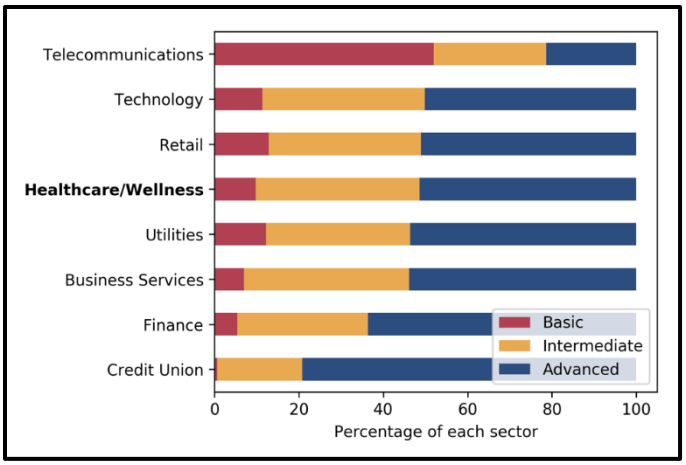


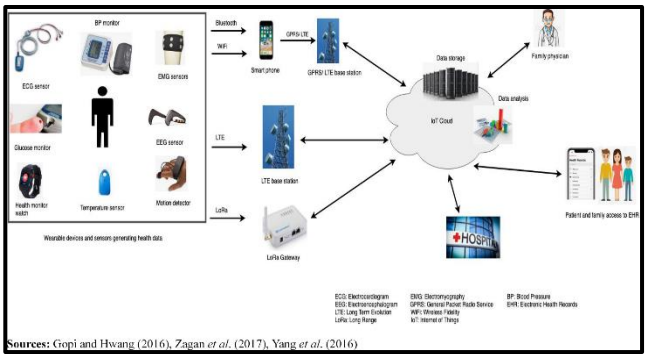
Figure 5 : Breakdown of Security Ratings by Major Industry.

IV. CHALLENGES

Due to the obvious attacks, the health business has faced several challenges and has been a key priority for a long time. The healthcare business has been under attack as a result of the public convergence of varied individuals seeking treatments. Since the majority of the content is still available on the websites for clients and patients to view, the attackers discovered a flaw in the company. As nothing more than a result, those with nefarious intents will find it easy to contact and collect information from them.

Because of not having confidentiality the healthcare is suffering in a major manner. The information which is sent among the different parties (patients and organizations) the technologies which are used for the data transferring is also very challenging. When looking at these challenges one of the main issues faced is keeping track of the data which are coming in and going out during the transfer of data among the different parties. Further getting the bet network is also one of the most challenging things the healthcare sector goes through because the information sharing methods are countless (payments, online clinics,) specially through the pandemic situation.

Also most of the IT professionals do prefer to play around with the dark web, because of some dislikes in their jobs. Further due to not having a proper training the employees have been facing many attacks from the black hat hackers



Sources: Gopi and Hwang (2016), Zagan *et al.* (2017), Yang *et al.* (2016)

Figure 6 : A smart health-care system.

VII. MITIGATIONS.

These issues and the dangers the healthcare sector faces due to cyber security should be solved immediately and for it all the stakeholders should cooperate to mitigate and prevent these attacks and difficulties; a better planning and implementing these plans are necessary to ensure that all the security methodologies are executed in a proper manner [21]. Further both parties from the government and the private sectors should works together and thrive through in order to establish processes which makes the security problems a non threat, and due to ignoring these factors the attackers have taken the upper hand, there are a number of effective protections that can help reduce the frequency of assaults. The following are some countermeasures; nevertheless, they are not all-inclusive:

Educating users: The client is the weakest link in either security system. People are viewed as the weakest link in many security systems. Client cybersecurity awareness via education programs is critical for lowering the risk of cyberattacks on an organization. According to the report, 11 percent of organizations intend to make security a high priority via planning, while the rest do not, demonstrating a significant disparity. However, in the fight against security, using an encryption platform to safeguard communication across a virtual private network has shown to be beneficial. Applicability, by use of a virtual private network (VPN) has now become part of the routine to many people. Using a VPN preserves your privacy and allows you to apply more appropriate regulations and security measures.

The security should be increased by the healthcare facilities to protect all types of sensitive data and the critical assets from the cyber-attacks. A firewall is a key component and also a intrusion detection system (IDS) which are mainly used for detecting unwanted activities which might make the network unworkable and jepordize it. To analyze the risks better the IDS uses a anomaly detection and test protocol analysis, such as deep pocket research and also some like matching the signatures. Also identifying the behaviors such as Zero day threats. , Artificial Intelligence outlier detection has made intrusion detection systems (IDS) the most common and accurate method of detecting attack

VIII. FUTURE RESEARCH.

Whereas the Internet has provided enormous benefits to the medical business, it has also created significant security issues. The purpose of this study was to use the Shodan database to detect vulnerabilities in networked medical equipment. Based to our first results, major suppliers such as Animas, Bionet, Roche, and ReliOn are vulnerable to Dropbear SSH server issues, PHP vulnerabilities, and OpenSSH weaknesses that allow remote code execution and/or authentication bypass.

Future work might take a variety of intriguing directions. First, by studying all of the medical equipment on Shodan, future research might significantly widen the scope of vulnerability assessment. Second, research may be conducted to determine who owns sensitive equipment so that the owners are aware of the hazards. Finally, to patch and secure the discovered vulnerabilities, automated mitigation procedures might be established. Plenty of the mentioned paths would help in the development of crucial medical device security capabilities [23].

Ongoing research routes should investigate reasonable and viable solutions to CSRF attacks in order to protect the operating devices. People must be aware of the hazard in order to defend the medical system. Moreover, because the bulk of inspections and processes may be greatly depreciated, solutions should focus on improving performance efficiency. DoS, backdoor, and ransomware attacks wreak havoc on data input and generation processes, interrupting them entirely or partially. Proposed approaches for achieving various goals have been offered; nevertheless, they are incompatible with the medical field.

As a result, enhanced detection methods for backdoors, DoS, and ransomware attacks are critical. The ransomware attack is particularly dangerous since present ransomware methods have poor system performance, which may alter the outcome. Intruders can change a patient's medicine dose using DoS and remote code execution, potentially leading to the patient's death. The majority of designs have been found to perform better in terms of transmission efficiency and data security. However, not all architectural concepts result in low pricing [24]. As a result, the planning and design routes are to generate less expensive designs. Health related frameworks that minimize expenses by offering lower-cost services will benefit patients and other medical staff.

IX. CONCLUSION.

This research does a comprehensive assessment of the literature on cyber risk in the healthcare business. It is a summary of the most significant cyber-risk research. It emphasizes the issue's importance. Additional research is required in this regard to solve the healthcare sector's vital infrastructure in order the field's future career prospects, whereas health facility research is insufficient to satisfy

healthcare demands. The primary goals of this review article are to increase awareness of the importance of the healthcare industry and to investigate the need for security measures in the healthcare sector to secure sensitive information in hospital databases. This article reviewed over 15 papers, but anyone may use this material to learn as much about the significance of this issue for public and government healthcare institutions.

Cybersecurity assaults have substantially affected the efficiency of the healthcare sector. As a result, more planning and effective channels for implementing plans are necessary to guarantee that all security systems are correctly assessed in order to protect the safety and confidentiality of health information in hospital databanks. Cyberattacks should be seen as a severe threat to all businesses, not only the healthcare industry. As a response, governments must ensure that adequate funds are committed to hospital firewalls and overall security.

The 2 emerging technologies IOT & SDN mainly handles and deal with sensors and network connection management. Further these technologies interdepend among each other and must mainly overcome many difficulties, such as programmability, data management to make sure the customer satisfaction is gained. Several challenges in the traditional healthcare system can be solved by integrating the two technologies.

SDN is a revolutionary approach to changing network design through the use of technology. IoT in healthcare has the potential to enhance manageable networking in order to solve a wide range of issues.

X. Acknowledgment

Specially thanks go out to our Applied Information Assurance lecturer in charge Mr. Kanishka Yapa for his valuable mentoring and technical advice making us motivate to complete our work. Furthermore, in this occasion we like to mention our cybersecurity batchmates who provide their very valuable feedback and much appreciated guidance during this research.

References

[1] G. Kortuem, F. Kawsar, V. Sundramoorthy, and D. Fitton, "Smart objects as building blocks for the internet of things," *IEEE Internet Comput.*, vol. 14, no. 1, pp. 44–51, Jan. 2010, doi: 10.1109/MIC.2009.143.

[2] "What is Software-Defined Networking (SDN)? - Ciena." https://www.ciena.com/insights/what-is/What-Is-SDN.html (accessed Mar. 21, 2022).

[3] D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel, "Security and privacy for implantable medical devices," *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 30–39, Jan. 2008, doi: 10.1109/MPRV.2008.16.

[4] K. Sood, S. Yu, and Y. Xiang, "Software-Defined Wireless Networking Opportunities and Challenges for Internet-of-Things: A Review," *IEEE Internet Things J.*, vol. 3, no. 4, pp. 453–463, Aug. 2016, doi: 10.1109/JIOT.2015.2480421.

[5] I. F. Akyildiz, M. Pierobon, S. Balasubramaniam, and Y. Koucheryavy, "The internet of Bio-Nano things," *IEEE Commun. Mag.*, vol. 53, no. 3, pp. 32–40, Mar. 2015, doi: 10.1109/MCOM.2015.7060516.

[6] M. Masdari and S. Ahmadzadeh, "A survey and taxonomy of the authentication schemes in Telecare Medicine Information Systems," *J. Netw. Comput. Appl.*, vol. 87, pp. 1–19, Jun. 2017, doi: 10.1016/J.JNCA.2017.03.003.

[7] "IEEE Xplore Full-Text PDF:" https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7843009&tag=1 (accessed Mar. 25, 2022).

[8] Y. Meng, Z. Huang, G. Shen, and C. Ke, "SDN-Based Security Enforcement Framework for Data Sharing Systems of Smart Healthcare," *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 1, pp. 308–318, Mar. 2020, doi: 10.1109/TNSM.2019.2941214.

[9] A. Strielkina, V. Kharchenko, and D. Uzun, "Availability models for healthcare IoT systems: Classification and research considering attacks on vulnerabilities," *Proc. 2018 IEEE 9th Int. Conf. Dependable Syst. Serv. Technol. DESSERT 2018*, pp. 58–62, Jul. 2018, doi: 10.1109/DESSERT.2018.8409099.

[10] J. Zhang, L. Li, G. Lin, D. Fang, Y. Tai, and J. Huang, "Cyber Resilience in Healthcare Digital Twin on Lung Cancer," *IEEE Access*, vol. 8, pp. 201900–201913, 2020, doi: 10.1109/ACCESS.2020.3034324.

[11] G. Lin, S. Wen, Q. L. Han, J. Zhang, and Y. Xiang, "Software Vulnerability Detection Using Deep Neural Networks: A Survey," *Proc. IEEE*, vol. 108, no. 10, pp. 1825–1848, Oct. 2020, doi: 10.1109/JPROC.2020.2993293.

[12] S. Sharma, K. Chen, and A. Sheth, "Toward Practical Privacy-Preserving Analytics for IoT and Cloud-Based Healthcare Systems," *IEEE Internet Computing*, vol. 22, no. 2, IEEE, 2018.

[13] G. Lin *et al.*, "Cross-Project Transfer Representation Learning for Vulnerable Function Discovery," *IEEE Trans. Ind. Informatics*, vol. 14, no. 7, pp. 3289–3297, Jul. 2018, doi: 10.1109/TII.2018.2821768.

[14] R. S. H. Istepanian, S. Hu, N. Y. Philip, and A. Sungoor, "The potential of Internet of m-health Things m-IoT for non-invasive glucose level sensing," *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. EMBS*, pp. 5264–5266, 2011, doi: 10.1109/IEMBS.2011.6091302.

[15] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, Jul. 2018, doi: 10.1016/J.MATURITAS.2018.04.008.

[16] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of IoT: Applications, challenges, and opportunities with China Perspective," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 349–359, Aug. 2014, doi:

10.1109/JIOT.2014.2337336.
[17] L. Wu, X. Du, M. Guizani, and A. Mohamed, "Access Control Schemes for Implantable Medical Devices: A Survey," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1272–1283, Oct. 2017, doi: 10.1109/JIOT.2017.2708042.
[18] N. Taimoor and S. Rehman, "Reliable and Resilient AI and IoT-Based Personalised Healthcare Services: A Survey," *IEEE Access*, vol. 10, pp. 535–563, 2022, doi: 10.1109/ACCESS.2021.3137364.
[19] S. Van Rossem *et al.*, "Deploying elastic routing capability in an SDN/NFV-enabled environment," *2015 IEEE Conf. Netw. Funct. Virtualization Softw. Defin. Network, NFV-SDN 2015*, pp. 22–24, Jan. 2016, doi: 10.1109/NFV-SDN.2015.7387398.
[20] "Cybersecurity Attacks during a Pandemic: It Is Not Just IT's Job! | Medsurg Nursing; 30(1):65-66, 2021. | ProQuest Central." https://pesquisa.bvsalud.org/global-literature-on-novel-coronavirus-2019-ncov/resource/pt/covidwho-1095011 (accessed Mar. 24, 2022).
[21] P. Anantharam *et al.*, "Knowledge-Driven Personalized Contextual mHealth Service for Asthma Management in Children," *Proc. - 2015 IEEE 3rd Int. Conf. Mob. Serv. MS 2015*, pp. 284–291, Aug. 2015, doi: 10.1109/MOBSERV.2015.48.
[22] A. D. Wood *et al.*, "Context-aware wireless sensor networks for assisted living and residential monitoring," *IEEE Netw.*, vol. 22, no. 4, pp. 26–33, 2008, doi: 10.1109/MNET.2008.4579768.
[23] H. Kumarage, I. Khalil, A. Alabdulatif, Z. Tari, and X. Yi, "Secure Data Analytics for Cloud-Integrated Internet of Things Applications," *IEEE Cloud Comput.*, vol. 3, no. 2, pp. 46–56, Mar. 2016, doi: 10.1109/MCC.2016.30.
[24] A. K. Pandey *et al.*, "Key Issues in Healthcare Data Integrity: Analysis and Recommendations," *IEEE Access*, vol. 8, pp. 40612–40628, 2020, doi: 10.1109/ACCESS.2020.2976687.

Author Profile.

Osuni D. Abeywickrama is a third-year first-semester student at SLIIT, where she is pursuing a BSc. Hons Information Technology degree with a specialty in software development. in the field of cyber-security. It's her first time writing a review article in the subject of healthcare. Her research examines a variety of topics of cyber security.