A Review of Cyber Security Threats and Mitigations in the Healthcare Sector

IT20128272 – Ratnayake.R.M.K.G.
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
New Kandy Rd, Malabe 10115, Sri Lanka
it20128272@my.sliit.lk

***Abstract*— Over the past few decades, the healthcare sector has evolved to connect with information technology. Today, almost all areas of healthcare are digital, thanks to the rise of information technology and the Internet of Things (IoT) and Software-Defined Networks (SDN). For example, the medical monitoring devices in the Medical Internet of Things (MIoT) work by connecting to cloud services, servers, clients, and databases. These MIoT devices record certain measurements by continuously monitoring the condition of the patient and sending them to the database called Patient Record Management System. Every patient record is considered sensitive information and diagnosed as a patient health record. Therefore, it is essential to implement appropriate security requirements and measures to mitigate potential cyberattacks in the healthcare sector. Especially during the COVID 19 pandemic, the healthcare sector has to deal with challenges posed by cybersecurity threats and threats. In Italy, for example, the COVID 19 emergency had a severe impact on cybersecurity from January to April of 2020, doubling the absolute number of attacks, accidents and privacy breaches affecting businesses and individuals. [19]. Due to the heavy involvement of the Internet of Things (IoT) and Software-Defined Networks (SDN), this summary article mainly focuses on cybersecurity threats, and their mitigation in the medical field focuses on the Internet of Things (IoT) and Software-Defined Networks (SDN) objects.**

Keywords—IoT, SDN, MIoT, Cyber risks, Cyber-attacks, Blockchain, 5G Network

I. INTRODUCTION

Healthcare can consider a universal need that impacts everyone in society. The medical department is accountable for gathering, analyzing, and holding sensitive data while sharing it with healthcare professionals, patients, and other organizations. In addition, medical systems are forced to evolve with technological advances. Because of that reason, Healthcare organizations are attractive targets for threat actors because they store compassionate personal information (PII) [14] about members/patients [3]. This information also includes bank account numbers representing payment methods such as name, address, date of birth, date of death, social security number (SSN), health insurance identification number (HIN), and credit card details. Combined with demographic data, this provides medical cyber threat actors with sufficient information to steal their identity or commit health fraud [3]. In addition, personal information and associated records of one's health are an attractive option for cybercriminals because of their underground market value. IBM and the "Ponemon" Institute reported in 2016 that the data breaches that occur in the healthcare sector have increased since 2010 and are currently one of the most vulnerable sectors to cyberattacks worldwide [5]. Such attacks put the patient's identity and finances in jeopardy, disrupt hospital operations, and jeopardize the patient's health [14]. For example, in 2017, the UK National Health System hospital was hit by ransomware known as "WannaCry" [16], which caused incoming ambulances to be bypassed and treatment plans to be postponed due to a loss of access to the hospital information system [5]. Furthermore, cyberattacks harm hospitals and medical facilities' reputation [14] and profitability and the operational delays and economic costs of data breaches and ransomware attacks.

The M8 Alliance has evaluated the breadth of cyber-attacks against hospitals in response to these global attacks. An interdisciplinary team of specialists conducted many conference calls based on the findings of this review. Following that, a workshop was organized in April 2018 at the Geneva Health Forum (GHF), held every other year. The goal of these gatherings was to share threats identified, foster interdisciplinary conversations, and provide practical suggestions to hospitals around the world. In addition, the World Health Summit Experts Conference on Hospital Cybersecurity [5] was hosted on-site at the GHF.

This review paper is mainly focused on IoT and SDN usage in the Healthcare Sector, the challenges/ cyber risks and threats that have arisen because of the involvement of the IoT and SDN in the Healthcare sector, and also the mitigation methods to avoid and mitigate those risk and challenges to make digital healthcare sector more secure place for sensitive information.

II. RESEARCH STATEMENT/ OBJECTIVES

There are areas in the healthcare industry that need to be improved to combat the recent increase in attacks, such as phishing and ransomware attacks, which attackers have used to exploit vulnerabilities in the Internet of Things (IoT) and Software-Defined Networks (SDN) in the healthcare sector. According to medical utilization of the Internet of Things (IoT) and Software-defined networks, this research aims to identify essential cybersecurity threats and mitigation approaches in the healthcare industry (SDN). Furthermore, this review article focuses on future research that will focus on medical applications of the Internet of Things (IoT) and Software Defined Networks (SDN).

III. REVIEW OF THE LITERATURE

Technology in Healthcare sector

The healthcare industry is changing rapidly with the development of information technology. Medical technologies have many advantages. Nowadays, smartphone apps, telehealth software, and SMS help improve communication between doctors and other healthcare

professionals and their patients and other healthcare providers [9]. Additionally, younger generations use “digital health” apps and patient portals to check test results, schedule appointments, and renew subscriptions [9]. In addition, healthcare facilities are improving their operations, leading to better care delivery, a more efficient workforce, and lower costs [9]. However, technology can also be a pain point if left unprotected. Therefore, it is essential to adapt to digital trends, meet patient preferences, and reduce security risks by eliminating the weaknesses that Cybercriminals seek to target.

A. Internet of Things (IoT)

The Internet of Things (IoT) has grown in recent years and has grown even more rapidly over the next few years. Nowadays, IoT has become the center of technological progress in all possible industries. That may seem like an exaggeration, but it is unlikely that the industry will spend the day without encountering the IoT.

Definition for IoT

The Internet of Things (IoT) is a network of physical items that use sensors, software, and other technologies to connect to other devices and systems over the Internet and exchange data [20]. These gadgets include everything from common domestic goods to complex industrial machines. There are currently around 7 billion connected IoT devices, with analysts predicting that figure to rise to 10 billion by 2020 and 22 billion by 2025 [20].

How does IoT work?

The Internet of Things (IoT) is a collection of web-enabled intellectual appliances that can gather, send, and respond to data from their surroundings using embedded techniques, including processors, sensors, and communication hardware. IoT devices also include sensors for data collecting and transmission, connected to IoT gateways or other edge devices. Then, by uploading the data to the cloud, it will be used for analysis. IoT devices can also communicate with other systems' drives to transfer data. These gadgets do not require human interaction to carry out their tasks, but they require human interaction to set up, deliver instructions, and retrieve data. These web-enabled devices' connectivity, network, and communication protocols are all largely dependent on the IoT application implemented for them. The Internet of Things (IoT) can also use artificial intelligence (AI) and machine learning to make data collection more straightforward and more dynamic [21].

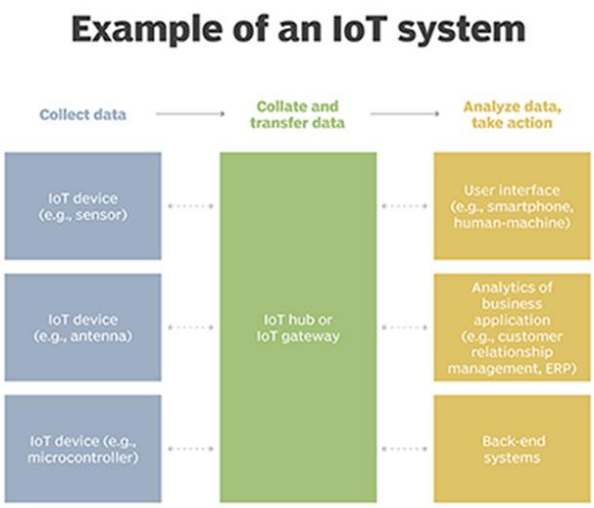

Figure 1: The process of IoT System

The importance of IoT

Better decision making

Additional sensors on these gadgets collect vast volumes of data of various characteristics. For example, instead of merely providing information about which foods are obsolete, "smart" refrigerators can send the user information on power usage, temperature, and average open-door opening time. More information flows means that the company that owns the device's technology can evaluate relevant trends in the data and improve its performance. As a result, most businesses see the value of this technology, which has resulted in the market's rapid expansion. By 2026, the annual value of the IoT market will approach $3 trillion [22].

Ability of monitoring and tracking in real-time

It keeps track of the information provided to the company, but it also benefits the users. These gadgets can track the quality of users' household goods in real-time. Knowing an item's state allows homeowners to know when to replace it without constantly inspecting its quality [22].

Automation for lighten the workload

Users can save more time and money by having a device that does most of the job. For example, consider having a new milk carton delivered when the one in the refrigerator expires. Furthermore, this will significantly reduce human labor. It also leads to the development of entirely self-contained gadgets that require little or no human interaction [22].

Improvement of efficiency

Not only do IoT devices save time, but they also save money. For example, users can save money by shutting off the electricity automatically when they leave a room. As a result, the connected gadget can deliver a wide range of valuable functions. In addition, the IoT system enables machine-to-machine (M2M) communication, which improves long-term efficiency for both businesses and users [22]. According to the growth rate of machine-to-machine communication, the overall number of connections will expand from 5 billion in 2014 to 27 billion in 2024 [22].

Better quality of life

All of the previously listed advantages contribute to a higher quality of life. Users can reliably minimize stress by having their devices track and order items, turn off lights, and perform time-sensitive tasks. The general populace will, without a doubt, get busy over time. Because numerous devices have evolved and new technologies have been deployed, tracking has become more complex. It is fantastic that people can do what they want while their computers take care of mundane tasks. The IoT's future also includes lifestyle enhancements, health benefits, and well-being enhancements [22]. A frequent exerciser, for example, can utilize wearable technology to track heart rate, temperature, and hydration to stay healthy and track their progress [22].

B. Internet of Medical Things (IoMT)

There are clear distinctions between the Internet of Things (IoT) and the Medical Internet of Things (MIoT). The Internet of Things (IoT) is a collection of billions of connected gadgets that use the Internet to collect and distribute data. Refrigerators, vehicles, smartphones, airplanes, and thermostats are among the gadgets and primary sensors that

make up the Internet of Things [15]. IoT allows web-connected devices to become almost self-sufficient and intelligent at the terminal level. They can use endpoints to analyze and process data without manual human intervention. IoT is broad since it encompasses all objects connected to the Internet.

On the other hand, the IoMT, also known as the Internet of Things or MIoT, can improve and optimize medical care by using solely Internet-connected equipment. Only users who require 24-hour follow-up and specialized supervision may benefit from this [15]. Furthermore, embedded technology differs between IoT and IoMT in that IoT is designed to fulfill any function in their respective organizations, whereas IoMT strives to improve healthcare delivery. The differences between IoT and MIoT are compared in the table below.

	IoT	IoMT
Use Cases	IoT covers a variety of new technology solutions used in many industries, including construction, industrial environments, and at home	IoMT features connected devices used in the medical and healthcare sectors
Design	IoT is consumer-focused and is designed to provide maximum usability and convenience.	IoMT is designed to provide reliability, accuracy, and enhanced security
Target customers	A majority of IoT branded devices target average customers. They do not require additional skills to operate	IoMT requires additional knowledge to interpret the device's operations and data
Regulations	General application IoT is less regulated	IoMT faces strict security protocols and HIPAA compliance

Figure 2: Differences between IoT and MIoT

Impacts of Utilizing Unsecured IoMT Devices [15]

Using IoMT devices while an impacted person's data is not always safe can harm all stakeholders in the healthcare industry. The healthcare industry heavily relies on statistics, which implies that if data is compromised, it could impact subsequent operations and intervention tactics. A compromise of healthcare data security could result in a loss of privacy and confidentiality and incorrect prescriptions, diagnoses, and treatment options. These findings could have negative clinical repercussions or be the cause of death. Furthermore, if IoMT devices are not secure, sensitive data about impacted people are vulnerable to illegal access and hacking.

Furthermore, cyberattacks might expose a victim's personal information, exposing them to the risk of being utilized for nefarious purposes. Another consequence of employing insecure IoMT devices is that availability, a vital aspect of information security, may suffer. The information gathered and retained by IoT devices must be available to felony investigators. However, this cannot be guaranteed where devices are vulnerable to cyber-attacks. For example, one cybercriminals' favorite pastime is erasing vital statistics, making them inaccessible to those who require them. In this instance, physicians and extraordinary clinical practitioners cannot be sure they will be able to acquire sufficient access to the patient's data through unprotected gadgets. Furthermore, such gadgets will not be dependable, as insufficient access might stymie service delivery and have disastrous effects.

C. Software-Defined Networking (SDN)

SDN is a programming method that manages virtual network devices with centralized management control panels via open interfaces in the most basic form of control. By moving information and packages from network devices spread to centralized controllers, network architecture, configuration, and facilitated programming ability, Software-Defined Networks have advanced routing algorithms [23]. This software-centric controller controls individual devices and online traffic flows, which leverages the OpenFlow or Male protocols. As a result, network engineers may control and administer network applications, often known as "Northbound applications," in an automated manner. Topology management, congestion control, service/chain insertion, load balancing, quality management service, firewall monitoring, and automation storage are some of the applications in Strategic areas [23]. Because patient information is spread across several healthcare contexts, a closed management system for management and service quality is required to communicate information. However, several conditions must be met. The network must be adaptable, virtualized, and integrated with high performance to overcome disaster and maintain business continuity. The combination of SDN and NFV enables the construction and automation of several virtualized network versions inside a portion of traditional networks [23]. Virtual appliances operate as traffic managers and load balancers in a virtualized environment, directing users to the right data center across different computing resources. Virtual machines can travel between physical entities or data centers, allowing safe cross-platform cloud data access. Each virtual instance can be delegated to each endpoint for patient monitoring, unified communications, electronic health records, and clinical data in a specific healthcare context. Each sector is equally vital, and they all require a stable connection and high-quality service to stay operational.

D. IoT/MIoT usage in Healthcare Sector

a) Artificial intelligence [15]

In healthcare, artificial intelligence is a critical component of the IoMT. Artificial intelligence in healthcare helps doctors investigate trends ranging from learning about patient activities in connected devices to tracking and analyzing patient transactions, allowing healthcare practitioners to provide preventive care. AI-based prophylactic healthcare models have been established due to breakthroughs in artificial intelligence in healthcare. Furthermore, AI in healthcare is advantageous since it establishes a system from which the healthcare system can continually learn, allowing healthcare providers to deliver care based on a patient's treatment history and medical records and develop new treatments. Artificial intelligence allows for the digitization and automation of medical knowledge acquired from various sources, including connected equipment, healthcare workers, nurses, and doctors. The synthesis of all gained knowledge makes it easier to provide the best possible medical care.

b) Healthcare Value Streams Digitization [15]

They have a suitable data recording procedure and digitization in end-to-end patient value streams. Furthermore, most healthcare institutions concentrate on optimization and efficiency to strengthen their control over dynamic case management and intelligent business process management. As a result, healthcare institutions routinely undertake repetitive operations and upgraded or automated activities through the application of artificial intelligence, such as entering and storing patient data. Cognitive work, knowledge work for

nurses and doctors, and AI-powered work for the staff: medical and other medical-related products are other categories where digitalization of value streams has dramatically improved. All three components can be used to create medical items using various IoT devices. For example, joyful monitoring allows doctors to watch good monitors temperature, blood pressure, and heart rate speed to monitor their patients' physical health. Sensors, smartwatches, and Fitbit devices are examples of IoT devices used for such purposes. They also apply to provide geriatric home health care. Adults choose to live in their own houses rather than hospitals or rehabilitation centers, so they have telecommunications and connection monitoring equipment at home.

Furthermore, the categories mentioned above of IoMT led to the creation of intelligent hospitals. IoMT device connections have a wide range of practical and pragmatic applications that contribute to intelligent hospitals' overall operation and operation. Other vital IoMT applications include, but are not limited to, keeping the number of hospitals and medical equipment up to date.

c) IoT Medical Devices and Connected Wellness [15]

IoMT Component for Connected Health and Internet of Things Medical Devices focuses on digital health technologies with a more consumer focus. Because innovative solutions are constantly developing to treat, monitor, and diagnose diseases, it helps Digital health technology evolve. In addition, to provide quality and optimized healthcare services, the IoMT devices are becoming increasingly connected and intelligent and continuously developing to be more powerful. Therefore, the importance of the development and advancement of the Internet of Medical Things and the connection between medical devices integrate information technology to provide exceptional medical services. Medical devices' information technology opportunities include improved storage, administration, and recovery of patient data, remote healthcare delivery and monitoring, and treatment delivery. In addition, they are advanced for patients suffering from adverse medical conditions.

E. SDN usage in Healthcare Sector

Entities withinside the Healthcare area presently address Wi-Fi connectivity assisting cloud programs, Internet of Things (IoT) gadgets, and telehealth applications, all strolling at the identical Wi-Fi community. All these visitors doubtlessly result in sluggish connections because of overloaded bandwidth and bottlenecking, resulting in clinicians not being able to get admission to mission-important gear on the care factor. Networks are increasing and assisting extra gadgets, and as they expand, the more challenging they are to manipulate. Large healthcare corporations are confronted with infinite switches and routers that want to be maintained personally and are not dynamic sufficient to vary community visitors primarily based totally on an organization's desires.
Software-described networking (SDN) can assist save you those problems. Software-described networking strips away the complexities of Wi-Fi hardware by consolidating control capabilities right into a control server that dictates how facts act via the community, permitting IT directors to preserve extra manipulation over their networks and reply to needs their networks extra quickly [24].

Healthcare Wi-Fi networks are complicated to manipulate because Wi-Fi networks assist numerous styles of facts. Organizations want if they want to prioritize alerts primarily based totally on their beginning and purpose. Healthcare is particular in that a break-up 2d of behind schedule conversation can doubtlessly have effects for an affected person. SDN facilitates corporations to cope with this trouble from an infrastructure standpoint [24]. SDNs permit IT departments to architect a custom control community, prioritizing specific packets relying on a hard and fast of dynamic factors. IT directors can prioritize visitors for special mission-important programs that save low precedence visitors, including back-workplace and private programs, from gaining precedence transmission via the community. The community desires to distinguish between a clinician searching at an affected person's file throughout a routine checkup and a clinician searching at an affected person's file within the ICU or emergency room. The community desires to decide which motion is extra urgent.
SDNs also are precious for healthcare corporations dealing with numerous deployments of linked gadgets [24]. The persisted adoption of IoT gadgets drives the want for an elastic community. According to the IEEE, SDNs assist higher manipulating and revealing bodily gadgets, which help corporations collect, transmit, and process facts [24]. Organizations can use those facts to construct higher IoT programs. The extra efficaciously the community can make manner and talk IoT facts, the extra precious it is to construct programs.
Many clinical IoT gadgets can shop a few affected person's information; however, the tool desires important and prioritized connectivity while alerts change, and the tool desires to alert an issuer to a critical situation.
For example, if a coronary heart reveal detects a life-threatening cardiac abnormality, facts should be prioritized while being transmitted to an issuer.
SDNs additionally assist telehealth applications [24]. Telehealth applications depend closely on robust community connectivity to ensure clinicians and sufferers can change facts appropriately and quickly. Clinicians broadcasting dense audio and video to a faraway place want a bendy community to make sure that every packet is delivered and each event sends and receives clean alerts.
SDNs are also helpful for fact migration and shifting huge documents, including clinical images [24]. IT directors can manipulate how much.

F. Emerging trends in cybersecurity risk

Cyberattacks can strike any network link or endpoint device. As a result, managing security concerns is critical, and software interoperability, operating platforms, medical device interfaces, and information exchange networks are all essential components of a digital health system. Because of the advent of physical medical cyber-flows, wireless connectivity, and the origin of medical applications in healthcare, the attack surfaces, and vectors in the healthcare industry have grown dramatically. Unfortunately, protecting every point of access to the healthcare system is impossible.

- ***Medical cyber-physical systems***

The Internet of Things (MIoT) and embedded and wearable medical devices for medical applications are included in this phrase. In addition, hospitals provide high-quality medical treatment through the Medical Cyber-Physical System (MCPS), a networked physical health system emerging as a promising platform for monitoring and controlling many aspects of patient health. By 2020, there will be 20 billion linked devices, with 50 billion by 2028 [2]. The unique qualities of MCPS, on the other hand, heighten the inherent security vulnerabilities. Because of these characteristics, MCPS is unlimited, portable, heterogeneous, and more ubiquitous. However, they are frequently isolated, with built-in devices for recording personal physiological data, limited size, performance, storage capacity, and only basic security features [2]. As a result, the MCPS functionality exposes users to security risks. In short, connecting and trusting the healthcare network raises the overall healthcare system's cybersecurity risk. As a result, MCPS has evolved into several potential attack channels through which hostile attackers can penetrate, install malware, and change treatments [2].

Cybersecurity measures like vulnerability screening and patch management are unavailable or only available from the vendor. MCPS aftermarket ownership, software updates, and safety requirements are unknown [2]. Manufacturers may be hesitant to release paperwork regarding device cybersecurity vulnerabilities, patching, and upgrade plans since it is personal knowledge. Incompatibilities between medical systems and devices increase due to a lack of medical standards to facilitate MCPS interoperability. Allowing healthcare providers to sell patient devices before resolving cybersecurity concerns helps develop markets [2]. Medical device cybersecurity vulnerabilities and a lack of vendor and regulatory monitoring should be strategic priorities for the sector.

- ***Data confidentiality, privacy, and consent***

The usage of personal data and the protection of sensitive patient data were listed as the following sub-topics. Medical confidentiality, accessibility, and integrity are tied to data belonging to every person in the healthcare industry and other associated data, and cybersecurity threats to those data can be categorized as medical confidentiality, accessibility, and integrity threats. Furthermore, the loss of personal health information and data and consumer trust, denial of service (DoS) threaten privacy, and ransomware assaults compromise access to patient records, software platforms, operating systems, and hardware [2]. Furthermore, the integrity of health data is jeopardized if data is damaged, erased, or manipulated, or if wireless connectivity with virtual devices or displays is hacked. Due to its sizeable economic scale and excellent attack area, health care is a vulnerable and appealing target for network assaults. With the importance of user information held in health care information systems in the health and nature sector, expanding the medical field's focus on network security is vital. Health and pharmaceutical data are significant assets for patients, healthcare providers, and identity thieves. Health data is 10 to 20 times more valuable than credit card and bank data [2]. Furthermore, credit cards or bank information may differ in flight cases: there is no history or identifying health information.

- ***Cloud computing***

Cloud computing is primarily employed in the healthcare sector for data storage, and it has been flagged as a cybersecurity concern for that data. Furthermore, because of the vast volume of medical data, storing, encrypting, deploying, and maintaining centralized data at the individual and organizational levels has become prohibitively expensive [2]. As a result, the advent of cloud computing has enabled data storage, processing, and analysis to be outsourced to a remote server. As a result, cloud models share data access, administration costs, and cybersecurity concerns [2]. Furthermore, because of the scale and efficiency of cloud computing, any data breach could be exposed to a larger audience [2]. With cloud storage, there are two possible attack vectors [2]:

1. attacks against data at rest, modifying or replacing information
2. attacks against data in motion, occurring

Encryption technology is required when sending to or from geographically distributed cloud servers to protect the security of patient data records while they are stored in the cloud. If the host operating system is hacked, attackers could access hypervisor processes and services, such as virtual machine monitors, computer software, firmware, or the hardware that generates and runs the machine [2].

- ***Health application security***

The extensive usage of healthcare apps and the lack of privacy protections pose a significant cybersecurity risk to personal data privacy and the integrity of facility infrastructure. Health apps can create, store, and process large volumes of identifiable health data. WhatsApp is popular among healthcare professionals because of its all-presence, simplicity, low cost, and advanced encryption, making it ideal for telemedicine services in resource-constrained environments and the facilitation of specialized networks [2]. WhatsApp is already so popular among doctors for professional and team communication that mandatory counseling is required to ensure that professionals do not mistakenly violate a patient's privacy or confidentiality [2]. Health departments recommend mental health apps as a safe, accessible, and economical alternative to face-to-face therapy, but there has been an investigation into the safety and security of such mental health and medical practice apps [2]. According to recent Australian research, more than half of government-approved apps lack a privacy policy that informs users about how their personal information will be handled and stored [2]. In addition, application developers frequently overlook patient privacy and security, or communications security is only examined for content, authorship, and trustworthiness. The author of a cross-sectional poll looking into the privacy and security of health apps on wearable devices discovered that respondents were unaware of privacy and security issues. Their mobile applications collect data, including what is obtained and how it is transferred or stored. According to the authors, these findings reflect the public's lack of awareness of potential data security and privacy threats. The government has approved these apps for people with dementia and mental illness. As a result, healthcare requirements can be exploited actively and passively without robust security rules, resulting in data change or theft [2].

- ***Insider threat***

The issue of insider threats is not fully discoursed in the cybersecurity tools in the healthcare sector as the ransomware "entry point" was the last sub-topic to be identified. Most data breaches involve intentional or unintentional internal cooperation [2]. Phishing emails have become a serious issue, especially during the COVID-19 pandemic, because of the inability of the healthcare sector to recognize or respond to those phishing emails, and it has become the most common way of healthcare sector security breaches. Most internal problems are caused by ignorance rather than malice, but random errors can also be damaging, making health and hygiene IT ignorance a problem and become difficult and become a severe threat [2]. Recent studies show that users in the healthcare sector are unaware of weak or insecure passwords, and there are no proper security measures to force them to use more robust and secure passwords either also, users are unaware of data breach procedures. Malicious intent associated with cyberattacks is not well understood, and the integration of human factors into the cybersecurity risk assessment is necessary to understand and characterize its policy impact to be reduced and fully minimized [2]. Inadvertent information leakage is inevitable due to the many risks of sharing cooperation in complex healthcare network systems [2].

G. Key security challenges and vulnerabilities in Healthcare sector

Analysis shows that the following issues are the biggest cybersecurity challenges in the healthcare sector [1].

1. Ensuring security when working remotely
2. Managing endpoint devices
3. Human error
4. Lack of security awareness
5. Inadequate top-level security risk assessment
6. Inadequate business continuity planning
7. Lack of coordinated response to incidents
8. Limitations beyond budget and resources
9. Healthcare system vulnerabilities

The healthcare sector's challenges and security concerns arise more than ever during the COVID 19 pandemic. Healthcare institutions must be aware of these challenges and take action to prevent them.

1. Remote work security assurance

During the COVID-19 pandemic, most organizations encourage their employees to work from home and define it as working remotely. The workers in the healthcare sector are also started remort working, and it has become an integral part of the healthcare sector. To access the organization's internal network, employees can use remote desktop protocols and virtual private networks (VPNs) [1]. However, there are known vulnerabilities in these remote desktop protocols and VPNs with certain risks contenders seek to exploit. For example, there are some security-related problems in the Remote Desktop Protocol, and it is not publicly available without additional protections such as firewalls, allowlists, and multi-factor authentication [1]. Furthermore, VPNs have particular client-side and server-side vulnerabilities that have been exploited by cybercriminals for years [1]. In addition, DDoS attacks on healthcare systems and countless wirelessly connected devices have created new challenges for the remote work environment [1].

2. Endpoint device management

In the healthcare industry, most endpoints are connected to the Internet or legacy dispersed networks that are unprotected or unpatched [1]. Furthermore, during the COVID-19 pandemic, many enterprises are tempted to buy more and more IoT devices, and more and more employees are tempted to work from home using their own devices, increasing the danger of cyber-attacks [1]. From an enterprise architecture standpoint, tighter integration into the information technology (IT) environment is beneficial; however, integrating new endpoints with older, older, or unsupported operating systems compromises interoperability and increases network security vulnerabilities like email phishing, ransomware, DDoS attacks, and network data breaches [1]. On the other hand, organizations place far too much reliance on perimeter defenses like antivirus, firewalls, and other critical cyber-attack defenses. As a result, endpoint complexity has the most influence on hospital security [1].

3. Human factors in cybersecurity

According to existing studies, human errors are to blame for most information security incidents [1]. When employees are busy saving lives and adapting to new work settings and technologies, human error is more likely to occur. In addition, employees are subject to malicious minions' of early work and errors due to abrupt changes in how we work and sustained exposure to stress. Workloads, for example, have a statistically significant positive relationship with the risk of healthcare personnel opening phishing emails [1]. Cybercriminals utilize social engineering techniques to exploit a human mistake in healthcare. This threat has grown more than ever during the COVID 19 epidemic. However, the healthcare industry has no root cause analysis to address safety hazards connected to human error, particularly those produced by inadvertent human mistakes [1]. Although some attempts have been made to evaluate the human error in applying human reliability analysis methodologies in information security, this approach has not been extensively accepted.

4. Lack of security awareness

Due to the low-risk impression of the healthcare industry and the most typical action performed in reaction to breaches or attacks, cybercriminals exploited people's worry during the COVID19 epidemic [1]. The most perplexing aspect is staff training or further communication. Healthcare personnel are unaware of the repercussions of some behaviours, and there are no policies or practices in place to encourage them. However, the healthcare industry must boost cybersecurity knowledge to safeguard themselves and their patients from cyber dangers like phishing and ransomware [1]. Healthcare personnel require greater training and assistance, such as pandemic-specific cybersecurity training campaigns, written protocols, and advisory guidance on updated processes and technology, due to a lack of preparation and training to work in pandemic scenarios [1]. Healthcare personnel, for example, must be aware of phishing emails containing pandemic buzzwords like "WHO" or "donate" and be able to report them [1]. They should also be instructed to avoid ransomware attacks by validating reliable information sources.

5. ***Inadequate board-level risk assessment communication***

Security risks and their influence on risk management across the company, such as the impact on patient care and clinical outcomes, are poorly understood. The healthcare sector lacks a matrix that can transform healthcare systems' strategic improvement goals into priority information / cyber improvement needs, and healthcare executives are uninformed of the impact of cyber intrusions on their business risks [1].

6. ***Inadequate business continuity plans***

The healthcare industry lacks adequate data protection safeguards. In comparison to other businesses, the healthcare sector, for example, lacks effective data security solutions [1]. Furthermore, neither the supply chain nor third-party providers have security built-in. According to existing studies, existing studies, vendor dependencies, poor encryption setups, and the inability to handle sharing and exchanging health information with third-party providers and cross-border partners are all important security issues, according to existing studies [1]. The dangers will continue to escalate unless cybersecurity is integrated into the project life cycle from the start. As a result, cybersecurity capabilities are a strategic asset that every healthcare organization should employ, as they help an organization create resilience and recover from incidents, learn from mistakes, and ensure business continuity.

7. ***Lack of coordinated incident response***

The healthcare industry has a history of a long period between an attack and its detection, which gives attackers more time to examine the network and move around, increasing the harm caused by security breaches. Current healthcare cyber defense solutions are usually reactive and established in the aftermath of malicious attacks, and they lack a coordinated incident response capability to tackle rapidly developing malware threats [1]. Furthermore, failure to develop a robust and secure backup strategy makes healthcare organizations subject to incident response and recovery [8]. Cybersecurity should be a collective endeavor from the board of directors to the front-line employees.

8. ***Limited budget and the need to deliver health care services without disruption***

Although healthcare organizations are spending money to become more connected in order to provide services without interruption, the security side of upkeep, such as keeping software updated and systems secure, is not getting the attention it deserves [1], reportedly leading to a lack of knowledgeable cybersecurity experts within healthcare systems with the necessary skills and experience to enable them to change their business operations at a rapid pace without unintended consequences [1][8].

9. ***Vulnerable MCPS***

Manufacturers are frequently unable to implement cybersecurity procedures such as vulnerability scanning or patch management. They are vulnerable to compromise because of their restricted core capabilities [1]. Vulnerability scanning and patch management, for example, are frequently inaccessible or only provided to manufacturers. Furthermore, their connectedness and reliance on the hospital network greatly raise the whole healthcare system's cybersecurity risk. Vulnerable IoT medical devices can introduce cyber vulnerabilities into medical network control systems due to their widespread adoption [1].

H. Common Cyber-attacks

Criminals and cyber-threat actors strive to exploit vulnerabilities associated with these shifts as the healthcare industry continues to supply important services while seeking to improve treatment and patient care through new technology. As a result, the healthcare business is dealing with many cybersecurity challenges. Malware that compromises system integrity and patient privacy and distributed denial of service (DDoS) assaults that interrupt the ability to offer care and patient care facilities [4] are examples of these issues. While attacks on other vital infrastructure sectors are common, the healthcare sector's mission presents its unique set of obstacles. Furthermore, hacks can have healthcare repercussions in addition to money loss and privacy infractions. Ransomware, for example, is a particularly dangerous type of malware for hospitals, as the loss of patient data can be fatal. Here are some examples of healthcare-related attacks.

1. Ransomware

The rapid increase in hospitals listed as ransomware victims is difficult to ignore. Ransomware is malicious software that infects computers and locks them up until a ransom is paid [10]. In healthcare, critical processes are hindered or even fully inoperable. Hospitals were forced to revert to pen and paper, which hindered the medical procedure and lost money that could have been used to update the facilities. Ransomware attacks a victim's computer in three ways [4].

1. via phishing emails containing malicious attachments
2. through a user clicking on a malicious link
3. by viewing ads that contain malware

Tactical, technical, and procedural (TTP) constantly changes, making security experts' jobs more difficult. Furthermore, platforms such as Ransomware as a Service (RaaS) make it simple for anyone with little or no technical knowledge to conduct ransomware attacks against the victims of their choice [4].

Several hospitals have recently been compromised with Ransomware due to old JBoss server software. Rather than attacking the hospital using conventional workstations used by personnel, the attacker placed the malware onto an obsolete server without the victim's knowledge [4]. Hollywood Presbyterian Hospital in California was one of the hospitals affected in a case that resulted in the hospital having to pay $17,000 to recover access to files and networks [4]. Regardless of the territory in which they operate, the actors employed an open-source application called JexBoss to search the Internet for vulnerable JBoss servers and compromised networks. Although there is no proof, some have argued that the high ransom demands in healthcare-related incidents indicate that cyber-threats know whom they have infected [4].

Furthermore, they may already know that equipment infected during an infection is typically crucial to a hospital's mission. Ransomware can make them unavailable, delaying patient care while putting immense pressure on the facility to fix the situation right away. This pressure, combined with the fact that hospitals frequently have the financial means to

compensate abusers, is likely to enhance the likelihood of abusers being compensated [4].

2. Data Breaches

Every day, another hospital makes the news that it is the data breach victim. It is common practice for individuals to receive a reassuring email of the breach and two years of free credit and identity tracking. According to the Ponemon Institute and Verizon Data Breach Investigations Report, the healthcare industry experiences more data breaches than any other industry [4]. However, this claim may be biased due to the clearly defined and legally mandated reporting requirements of the Health Insurance Portability and Accountability Act (HIPPA) [4] [13]. The law makes reporting violations in the healthcare sector more likely than violations in other areas.

Various incidents, including credential-stealing malware, can cause breaches, insiders intentionally or unintentionally leaking patient data, or losing laptops or other devices. Personal health information (PHI) is more valuable on the black market than regular credit card credentials or personally identifiable information (PII) [12]. As a result, cybercriminals have more incentive to target medical databases. They can sell PHI and use it for their benefit. According to the Health and Human Services Breach Report, more than 15 million health records have been compromised due to a data breach [4].

3. DDoS Attack

Distributed denial of service (DDoS) assaults are a famous tactic, technique, and procedure (TTP) utilized by hacktivists and cybercriminals. They can crush a community to the factor of inoperability, which can pose severe trouble for healthcare vendors who want to get entry to the community to offer the right affected person care or want to get entry to the Internet to ship and obtain emails, prescriptions, records, and information. While a few DDoS assaults are opportunistic or may be accidental, many goal sufferers for a social, political, ideological or economic purpose associated with a state of affairs that angers the cyber risk actors [4].

For example, in Boston Children's Hospital in 2014, a famous hacktivist organization called "Anonymous" centered the clinic with a DDoS assault after the clinic encouraged one in each of their sufferers, a 14-year-vintage girl, to be admitted as a ward of the kingdom and that custody be withdrawn from her dad and mom [4]. The docs believed the kid's disorder became a mental sickness and that her dad and mom have been pushing for useless remedies for a sickness the kid did now no longer have. The custody debate positioned Boston Children's Hospital with inside the center of this debatable case, and a few, including individuals of Anonymous, regarded this as an infringement of the girl's rights. Anonymous took motion via way of accomplishing DDoS assaults in opposition to the clinic's community, which led to others in that community, including Harvard University and all its hospitals, dropping Internet entry. According to the Boston Globe, the networks skilled outages for nearly a week, and a few clinical sufferers and clinical employees could not use their online debts to test appointments, check results, and different case information. As a result, the clinic spent extra than $300,000 responding to and mitigating the harm from this assault, in step with the attacker's arrest affidavit [4].

I. Recent Attacks

1. Lukaskrankenhaus Neuss (Germany)

Hospital Neuss (Lukaskrankenhaus Neuss) is a public hospital in Neuss founded in 1911 and has 537 beds and 1400 workers [5]. Employees received a variety of error messages in February 2016 due to ransomware attacks that used social engineering tactics [5]. The hospital pulled the server and computer systems down to assess and clean up the compromised system. Employees relied on pens, paper, and fax machines to keep functioning at this time, although dangerous actions had to be postponed. The hospital did not receive a direct monetary claim but provided an email address to contact for additional information. Following the recommendation of the local authorities, no attempt was made to contact the attacker [5]. According to the hospital, the backup system was kept up to date, and just a few hours of data were lost, but the backlog of handwritten documents from when the computer system was down was finally gone with the rest of the EHR. Integration is required [5]. According to a hospital official, it will take several months for the workflow to return to normal. There was no proof that the patient's information had been tampered with.

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

The Southeastern Norwegian Department of Health (SouthEast RHF) is a state-specific specialized hospital and medical services organization created in 2002 in collaboration with three other local governments [5]. SouthEast RHF revealed in January 2018 that roughly 2.9 million PHIs and records, or nearly half of Norway's population, were at risk [5]. Attacks on patient health records and the relationship of medical services with the Norwegian army are thought to have been spearheaded by foreign espionage or sophisticated criminal organizations of state agencies. A typical Windows XP system is to blame for this vulnerability [5]. The company had begun security procedures to limit the hazards posed by Windows XP and planned to phase it out, but the attack occurred before the security measures were put in place. Although the hack did not endanger patients or cause delays in hospital operations, it sparked concerns about future attacks on health data for political benefit and the GDPR. Therefore, it was a wake-up call. The GDPR required the company to notify the data subject within 72 hours, but it did not [5].

3. Hancock regional hospital (United States)

Hancock Regional Hospital, a small 71-bed non-profit hospital in Greenfield, Indiana, was founded in 1951 [5]. The malware "SamSam" [5] launched a ransomware attack against Hancock Regional on January 11, 2018. The attack was launched against the servers of an emergency IT backup system and spread via an electronic link between the backup site and the hospital's server farm, which is located a few miles from the main campus. Except for electronic medical record backup files, hackers were later revealed to be irreversibly corrupting backup file components of numerous systems. In addition, investigators revealed that the attack used Microsoft's Remote Desktop Protocol as an access point to the server and that the attack was launched using the hardware vendor's administrator account [5]. After the incident, the hospital has IT team took down all network and desktop systems.

Despite this, hospital operations continued during the shutdown. The hospital was not closed, and the patient was not diverted. The hacker requested four Bitcoins worth $ 55,000 as a ransom, which the hospital agreed to pay. The IT team then worked for three and a half days to decrypt the files and get the system up and running [5]. There was no evidence that patient information had been compromised. CEO Steve Long stated that the attack was a deliberate attempt by advanced criminal gangs to target medical facilities, and he released an article explaining her decision to pay the ransom [5].

During the COVID-19 Pandemic

Multiple cyberattacks happened in the healthcare industry at the onset of the global COVID 19 pandemic in early 2020. As a result, we chose a well-documented cyberattack with extensive details on the origins and repercussions. The most significant findings are reported in the table below.

Security incidents	Type of attack	Impact
US Department of Health and Human Services	Distributed denial of service	Disruption to COVID-19 pandemic responses
World Health Organization	Ransomware/phishing	Defacement and misinformation
Gilead Sciences, Inc	Phishing	Impersonation and exfiltration
Hospitals in Romania	Phishing/ransomware	Disruption and exfiltration
Health care supply chains	Malware	Disruption of activities
Brno University Hospital	Ransomware	Postponement of surgeries, appointments

Figure 4: Incident and the impact

The US Department of Health and Human Services

A DDoS attack was launched against the US Department of Health and Human Services to disrupt an organization's response to the COVID 19 pandemic [1]. The attack targeted the server, which bombarded it with millions of hits over several hours. It was described as a tumultuous effort to impede the response to the coronavirus epidemic since agencies responsible for preserving residents' health and providing essential welfare services were disrupted. The agency said that the attempt was unsuccessful and that the attackers did not get access to internal networks or steal data, but such attacks jeopardize health-care services and the lives of those who rely on them, implying that it could affect Emergency [1].

World Health Organization

The World Health Organization (WHO) should pay more attention to the general populace. As a result of the increased attempts to hack phishing websites targeting "WHO" and its partners, more than 4000 coronavirus-related domains have been reported to have been established since early 2020 [1]. For example, a hacker orchestrated the WHO case to collect credentials [1]. Furthermore, it has been alleged that a group of hackers developed a rogue website disguised as an email login portal for "WHO" staff to obtain passwords. The attempt failed, according to WHO, but it demonstrates that phishing attacks may be used to target medical organizations [1].

Gilead Sciences, Inc

Hackers also targeted Gilead Sciences, Inc., a manufacturer of coronavirus vaccines. A bogus email login page was used to obtain this pharmaceutical company's employees [1]. The incident was described as an effort to hack into firm employees' email accounts by sending messages posing as journalists.

Hospitals in Romania

In a Romanian hospital, a hacker launched a ransomware attack. Hackers planned to use COVID 19-themed email to infect these hospitals with ransomware. They were protesting the country's COVID 19 quarantine policies [1]. Remote-access Trojans, ransomware, website spoofing, and SQL injection tools were among the malware used by hackers to take down systems and steal data. In addition, they allegedly planned to send an email to the hospital regarding COVID 19 to infect computers, encrypt information, and disrupt hospital operations. The attack, however, was not as effective since Romanian law enforcement agents tracked down and apprehended the hackers [1].

Brno University Hospital

Brno University Hospital, one of the critical COVID 19 test centers in the Czech Republic, was hit by ransomware postponed surgery [1]. The ransomware infection was confirmed early when the hospital decided to disconnect all computer networks. It turned out that the ransomware infection was gradually replicated, and all individual systems went down. As a result, all computers had to be shut down. The hospital is reportedly recovering as it is not yet fully functional due to the attack [1]. The attack affected hospital activities because there was no database system or storage of data. As a result, employees had to manually write and copy their notes, which led to process delays and could endanger life in these times of trials.

I. Countermeasures of Healthcare sector

How to manage the risk in Healthcare sector [6]

There are several measures that the Healthcare sector can implement to manage risks successfully. Typically recognized security techniques such as,

- Identification and Authentication
- Security Patch Management
- Firewalls
- Encryption
- Standardized Policies and Procedures

Identification and Authentication [6]

Owners and operators can use identification and authentication procedures to identify system users and certify that data comes from a reliable source. Intrusion into cyber systems, loss of private information, and loss of service availability can all be prevented using identification and authentication. A comprehensive security strategy should be in place to protect the data, requiring anyone with access to authenticate their identities [17].

A Palmetto, Florida lady, for example, hacked into the Suncoast Community Health Centers, causing $17,000 in damages. The woman hacked into the computer system and "deleted and moved files, changed administrative account names and passwords, removed access to infrastructure systems, changed pay and accrued leave rates on the employee payroll system, and compromised the firewall used to protect the health centers' computer network," according to the report. Keep your systems up to date to stay on top of disgruntled employees, both past and present. In addition, the hacker gained access to information about the drugs prescribed to active-duty military troops, retirees, and their families.

Security Patch Management [6]

To repair existing problems or vulnerabilities, it is critical to upgrade the software package. Security patch management (SPM) decreases the risk of system failures compromising applications, systems, and PCs. To avoid the danger of future damage, updates should come directly from the software provider. After security patch updates, pre-programmed medical devices are at significant risk of crashing. According to Lynn Sherrill, since January 2009, 173 medical equipment have been infected with malware, deputy director of the Department of Veterans Affairs Health Information Security Division. Because security updates have the potential to damage or jeopardize medical devices, they should be extensively analyzed, tested, and prioritized before being used. In addition, if a software patch compromises the safety or effectiveness of medical equipment, the manufacturer must notify the FDA.

Firewalls [6]

Authorized users can access the computer's network system through firewalls. Using built-in filters can prevent potentially harmful material from entering the network while logging attempted breaches. The public Internet is the most critical threat to a firewall.

Firewalls use four different methods to restrict network traffic:

- packet filtering
- circuit-level gateway
- proxy server
- application gateway

The flow of information is limited by packet filtering, based on rules defined by the system administrator. The packet filter will examine incoming and outgoing packet headers. Depending on the source of information, the packet's intended destination, and the type of port used, packets are then allowed or rejected. Circuit-level gateways do not filter each packet, but they help maintain the private network's security by preventing the leakage of sensitive data. When a Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) connection is formed, circuit-level gateways employ security procedures. TCP and UDP connections are the Internet's principal communication languages or protocols. As a result, packets can flow freely between the hosts once the connection has been established. Proxy servers serve as security, administrative control, and caching intermediary between users and the Internet. A proxy server is a component of a gateway server, which divides the internal network from other networks, and a firewall server, which protects the network from outside incursion.

Encryption [11]

Encryption is the process of transforming data into code in order to safeguard it. The information can only be accessed by those who have this code. As a result, it is critical to think about the various encryption sorts to ensure they function with specific sensitive file transfer and sharing techniques. The majority of passwords used for file protection are poorly structured and easily cracked using commercial password recovery tools, according to a two-part study recently published in the Journal of Medical Internet Research titled "How strong are passwords used to protect personal health information in clinical trials?" At the Khaled ElEmam Research Institute of the Children's Hospital of Eastern Ontario (CHEO), the Canadian Research Chair led research on electronic health information. ElEmam decrypted fourteen of fifteen sensitive data supplied through email using commercial password recovery software. Thirteen of the fourteen records contained personal information such as date of birth and gender. According to research, customers are also in danger of identity theft if unencrypted patient information is transmitted over email or on shared files with shared passwords.

Standardized Policies and Procedures [6]

Standard policies and procedures should be used to establish the organization's requirements for security management, system performance, and security. In March 2011, for example, Massachusetts General Hospital was fined $1 million in court fees and fines for losing 192 patient records. A hospital billing manager brought the folders out of the hospital to work from home, but they were accidentally left on an MBTA subway train. The tapes were never found or recovered as a result. Since the hack, Massachusetts General Hospital has pledged to implement a "Correct Action Plan" (CAP) and fund employee training as part of the plan, which would include new processes for handling paper documents as well as data encryption on computers and other mobile devices in the event of a breach. In addition, to keep up with changing laws and technology, policies and processes should be reviewed at least once a year.

Other actions that can take to secure Healthcare sector

1. **Develop a risk-informed cyber strategy** [7]

The awareness should inform the organization's cyber risk management plan. First, assess the dangers to the facility's digital assets and potential security vulnerabilities. To make a successful shift, healthcare institutions must first organize themselves by creating a clear list of cybersecurity objectives and resources. If necessary, seek professional assistance during the procedure. The best way to conduct a risk assessment is to understand the assessment's aim and scope clearly. Organizations have a clear and practical means to achieve their goals in the face of change while retaining their priorities with the proper evaluation and plan.

2. **Actively monitor systems** [7]

If a hacker gains access to an organization's networks, it is critical to identify their movements and respond quickly. However, in healthcare organizations in Canada, a lack of rigorous internal oversight is expected. During our in-depth investigation, we discovered sensitive information from numerous facilities that had gone unreported, underlining the

importance of regularly monitoring systems for unexpected activity. Organizations should create playbooks and examine their internal processes to establish what alerts are created and what mechanisms are in place to monitor them in a breach. Get a clear picture of the data shared with other parties and handle all risks with contractual requirements while working with third parties. Monitoring can go a long way toward preventing damage from a breach.

3. **Improve security awareness among staff** [7] [11] Targeted phishing attempts pose a threat to healthcare businesses. During our investigation, some employees emailed us their login details, which we utilized to access their intranet. In which hackers breach into facilities and connect illicit devices for remote access to internal systems, the physical intrusion is also a risk for these companies. Staff must receive security awareness training to avoid falling prey to sophisticated assaults or allowing unauthorized employees access to sensitive places. Devote time and resources to educating, training, and supervising employees. Organizations should conduct phishing tests regularly to detect issues and subsequently provide training.

4. **Discover and act on vulnerabilities** [7]

Prior to hackers exploiting vulnerabilities and misconfigurations, identify them. Healthcare companies should do regular vulnerability assessments [18] to verify that the system is as operational as feasible. Penetration testing will also assist facilities in detecting the majority of vulnerabilities in their environment that could expose sensitive data to assault. In addition, penetration testing will aid in the identification of businesses that are exploiting vulnerabilities and configuration flaws. As a result, performing a vulnerability assessment before starting a penetration test is critical.

IV. FUTURE RESEARCH

Blockchain applications for Healthcare sector [25]

Blockchain is a relatively new and rising technology with creative uses when adequately used in healthcare. The development of cost-effective treatments and therapeutic approaches is aided by smooth and fast data sharing and dissemination among all central network members and healthcare providers. In the coming years, the medical business will be driven by complex treatments for various ailments. The advantages of Blockchain technology in the logistics business were recently disclosed, as were the benefits of Blockchain technology in the healthcare sector. Because this industry directly impacts people's quality of life, it is one of the first to benefit from digital transformation. Simultaneously, Blockchain technology is gaining traction, particularly in the financial industry. As a result, it presents the healthcare business with several significant and spectacular potential, ranging from science and logistics to physician-patient relationships.

5G Technology in Healthcare sector [26]

Continuous deterioration in the value for the patient, which is the relevant outcome for the patient divided by the cost per patient to obtain the result, leads to skyrocketing healthcare expenses. Furthermore, there are growing worries about the imbalance of health resources, ineffective healthcare management, and inconvenient medical experiments. To address these issues, technologies such as the Internet of Things (IoT), cloud computing, big data, and artificial intelligence are growing to improve patient experience and quality of medical services while lowering overall healthcare costs. Telehealth and remote patient monitoring, for example, reduce the time it takes for care providers to communicate with one another. Problems such as network congestion and sluggish internet speeds, on the other hand, constitute a serious concern, particularly for healthcare providers who may communicate with dozens of patients daily.

Furthermore, the widespread adoption of the Internet of Things (IoT) technologies will add to the current strain. The most significant influence on the healthcare scene will be 5G. The healthcare business is predicted to endure the most significant changes due to 5G's maximum bandwidth, low latency, low power, and cheap cost. Healthcare executives have discovered and deployed many connected care use cases, but mainstream adoption has run into constraints in existing communication technologies. Equal Reliable and high-speed connectivity will be critical as healthcare systems migrate to cloud-native designs.

High-speed data transmission, super-low latency (data delay responsive transmission systems), connection and capacity, high bandwidth, and durability per unit area are all qualities that 5G technology has the potential to solve. As a result, 5G presents an enormous opportunity for healthcare providers to restructure, convert to a data-driven holistic approach to individualized care, maximize medical resources, deliver convenient care, and add value to patients.

V. CONCLUSION

This review looks at the literature on cyberattacks in the healthcare industry that use the Internet of Things (IoT), the Internet of Medical Things (IoMT), and Software-Defined Networking (SDN). Cyberattacks against the healthcare sector are on the rise, owing to the lucrative patient data available in digital healthcare systems and the healthcare facility's ability to safeguard and receive poor knowledge of network security. In addition, out-of-date healthcare IT systems and a lack of cybersecurity engagement in the hospital industry are also challenges. Security concerns are missing from health management training, and the health system will remain vulnerable until this is addressed. Without essential cybersecurity skills training, healthcare executives will be unable to change the development of healthcare cybersecurity skills and workplace recovery. There is no way to avoid the danger of a cybersecurity incident or compromise in the healthcare system altogether. On the other side, developing a responsible healthcare culture regarding cybersecurity maturity can help to mitigate cybersecurity risks.

VI. ACKNOWLEDGMENT

Thank you to our Lecturer in charge, Mr. Kanishka Yapa, for giving us the valuable opportunity to undertake this project. I want to express my appreciation to all those who provided the resources and insight to complete this summary document quickly and meaningfully.

VII. REFERENCES

[1] Clemens Kruse, Andelka Phillips, "Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review," 2021.

[2] E. Sitnikova, K. Joiner, C. R. MacIntyre, "Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation," *Taylor & Francis Online*, pp. 556-585, 2020.

[3] H. Singh, "Healthcare Cybersecurity: Threats and Mitigation," infosecurity , 29 December 2021. [Online]. Available: https://www.infosecurity-magazine.com/blogs/healthcare-cybersecurity-threats/. [Accessed 25 February 2022].

[4] "Cyber Attacks: In the Healthcare Sector," Center of Internet Security, [Online]. Available: https://www.cisecurity.org/insights/blog/cyber-attacks-in-the-healthcare-sector. [Accessed 25 February 2022].

[5] Salem T. Argaw, Juan R. Troncoso-Pastoriza, Darren Lacey, Marie-Valentine Florin, Franck Calcavecchia, Denise Anderson, Wayne Burleson, Jan-Michael Vogel, Chana O'Leary, Bruce Eshaya-Chauvin & Antoine Flahault, "Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks," *BMC*, 2020.

[6] "Healthcare and Public Health Cybersecurity Primer: Cybersecurity 101," [Online]. Available: https://www.phe.gov/Preparedness/planning/cip/Documents/cybersecurity-primer.pdf. [Accessed February 2022].

[7] "Managing cybersecurity risks in the health sector," PWC, [Online]. Available: https://www.pwc.com/ca/en/industries/government-and-public-services/healthcare-cyber.html. [Accessed February 2022].

[8] "4 Healthcare Cybersecurity Challenges and How to Combat Them," CampusSafety, 17 November 2021. [Online]. Available: https://www.campussafetymagazine.com/hospital/healthcare-cybersecurity-challenges/. [Accessed February 2022].

[9] "4 Healthcare Cybersecurity Challenges," Maryville University, [Online]. Available: https://online.maryville.edu/blog/healthcare-cybersecurity/#modernizing-healthcare. [Accessed February 2022].

[10] Clemens Scott Kruse, Benjamin Frederick, Taylor Jacobson and D. Kyle Monticone, "Cybersecurity in healthcare: A systematic," Texas State University, San Marcos, TX, USA, 2017.

[11] S. Conaty-Buck, "Cybersecurity and Healthcare records".

[12] Anthony J. Coronado, Timothy L. Wong, "Healthcare Cybersecurity Risk Management: Keys To an Effective Plan," *Biomedical Instrumentation and Technology*, vol. 48, no. s1, pp. 26-30, 2014.

[13] S. Murphy, "Is Cybersecurity Possible in Healthcare ?," *National Cybersecurity Institute Journal*, vol. 1, no. 3, p. 68, 2015.

[14] Aurore LE BRIS, Walid EL ASRI, "State of Cybersecurity and Cyber Threats in Healthcare Organizations," ESSEC Business School.

[15] S. Z. Albaqami, "Threat Analysis for Healthcare IoT Devices," Flinders University, Adelaide, Australia, 2020.

[16] Panagiotis Radoglou-Grammatikis, Konstantinos Rompolos, Panagiotis Sarigiannidis, Vasileios Argyriou, Thomas Lagkas, Antonios Sarigiannidis, Sotirios Goudos and Shaohua Wan , "Modeling, Detecting, and Mitigating Threats Against Industrial Healthcare Systems: A Combined Software Defined Networking and Reinforcement Learning Approach," *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS*, vol. 18, no. 3, p. 12, 2022.

[17] Francesco Restuccia, Salvatore D'Oro and Tommaso Melodia, "Securing the Internet of Things in the Age of Machine Learning and Software-defined Networking," *IEEE INTERNET OF THINGS JOURNAL*, vol. 1, no. 1, p. 14, 2018.

[18] Derek Mohammed, Ronda Mariani, Shereeza Mohammed, "Cybersecurity Challenges and Compliance Issues within the U.S. Healthcare Sector," *International Journal of Business and Social Research*, vol. 5, no. 2, p. 12, 2015.

[19] Alberto Sardi, Alessandro Rizzi, Enrico Sorano, Anna Guerrieri, "Cyber Risk in Health Facilities: A Systematic Literature Review," *MDIP*, vol. 12, no. 17, 2020.

[20] "What is IoT?," Oracle, [Online]. Available: https://www.oracle.com/internet-of-things/what-is-iot/. [Accessed March 2022].

[21] A. S. Gillis, "What is the internet of things (IoT)?," TechTarget, [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT. [Accessed March 2022].

[22] Tim, "The internet of things (IOT): 5 reasons why the world needs it," Medium, 18 February 2019. [Online]. Available: https://medium.com/zeux/the-internet-of-things-iot-5-reasons-why-the-world-needs-it-125fe71195cc. [Accessed March 2022].

[23] H. MK, "The impact of SDN-IOT in the data rich Healthcare industry," Happiest Minds, 27 December 2017. [Online]. Available: https://www.happiestminds.com/blogs/the-impact-of-sdn-iot-in-the-data-rich-healthcare-industry/. [Accessed March 2022].

[24] E. O'Dowd, "Benefits of Software-Defined Networking in Healthcare," HIT Infrastructure, 16 June 2017. [Online]. Available: https://hitinfrastructure.com/features/benefits-of-software-defined-networking-in-healthcare. [Accessed March 2022].

[25] Abid Haleem, Mohd Javaida, Ravi Pratap Singh, Rajiv Suman, Shanay Rab, "Blockchain technology

applications in healthcare: An overview," *International Journal of Intelligent Networks*, vol. 2, pp. 130-139, 2021.

[26] S. Jadhav, "5G in Healthcare," TATA Elxsi, 2021.

AUTHOR PROFILE

Ratnayake.R.M.K.G.
BsC (Hons) in Information Technology Specialization in Cyber Security
Sri Lanka Institute of Information Technology
rmkgrathnayake@gmail.com