Major CyberSecurity Threats in Healthcare During Covid-19 Pandemic

Viet Minh Nguyen
Department of Computer Science
University of New Orleans
New Orleans, LA, USA 70148
Email: vmnguye2@my.uno.edu

Abdullah Yasin Nur
Department of Computer Science
University of New Orleans
New Orleans, LA, USA 70148
Email: ayn@cs.uno.edu

***Abstract*—The coronavirus pandemic created an unexpected crisis and changed all aspects of our lives. Specifically, country-wide lockdowns changed the working environment by replacing office work with remote work. Companies that were not ready for such transition experienced vital problems since the vulnerability of their system increased significantly. Vulnerabilities attract cybercriminals to deploy several types of sophisticated attacks to get financial gain, reputation, or hacktivism. During the pandemic, one of the main targets was the healthcare sector, where various healthcare institutions were targeted. Since healthcare is considered critical infrastructure in many countries, protecting sensitive information is crucial. Therefore, healthcare providers need to be prepared to respond to any cyber-threat and possible attacks. This paper outlines major cybersecurity threats focusing on the healthcare sector.**

I. Introduction

The uncertainty created by the Covid-19 pandemic drastically changed day-to-day life. Country-wide lockdowns increased the usage of the Internet significantly. Additionally, many organizations moved to fully remote working. The unexpected and sudden change in the working environment created big problems since most companies did not have previous plans and scenarios. In most cases, employees use their personal devices which are mostly unsecured. Moreover, most employees needed to connect their company servers to access information. Making servers and sensitive information accessible outside of a closed network creates additional vulnerabilities if necessary precautions are not taken.

The healthcare industry got a massive portion in terms of economic incentives. Many governments all around the world funded drug companies to develop a vaccination. Several relatively new companies became major players in the healthcare field. For instance, the market cap of Moderna was 6 billion dollars pre-covid, and it hit 195 billion dollars around August 2021. Many debates occurred regarding the patent waiver on Covid vaccinations to increase the manufacturing rate and make it more accessible to emerging countries. Since money and hacktivism are two primary motivations for many hackers, the healthcare sectors were the main target for cybercriminals during the pandemic. In June 2020, hackers targeted Moderna to steal the vaccine data. In January 2021, European Medicines Agency was targeted by cybercriminals, and hackers leaked Moderna and Pfizer's vaccine data.

The heavy spotlight makes most of the healthcare companies possible targets. It is quite easy to exploit possible vulnerabilities if those companies do not have proper defense mechanisms. Cyber attacks can create reputation problems, and the results can be costly for the victim. In case the company is publicly traded, the stock price may go significantly lower if the attack succeeds. Additionally, possible lawsuit penalties can go up to $500 million for sensitive data breaches [27]. It is crucial that healthcare organizations invest in the security of their network and implement an extensive defense mechanism, reduce possible vulnerabilities, and educate their employees.

In this paper, we review the significant cybersecurity problems in the healthcare industry during the Covid-19 era. We focus on Man-in-the-middle (MITM) attacks, phishing attacks, network attacks, 5G network attacks, and insider threats. We provide a taxonomy to break the problem into smaller parts to make it easier to follow. We highlighted the weaknesses and vulnerabilities of the healthcare providers which cybercriminals can exploit.

II. Taxonomy

People usually pay attention to the handling process of medical records considered sensitive data by HIPAA rule when focusing on Cyber security in healthcare. However, cybercriminals target all parts of healthcare organizations, such as networks, medical devices, and embedded systems. According to the Centers for Disease Control and Prevention (CDC), HIPAA stands for The Health Insurance Portability and Accountability Act of 1996 [28]. This federal law mentions the necessity of forming national standards to secure sensitive medical information of any patients in general. Moreover, it is also required to ask patient's consent or knowledge before disclosing anything. HIPPA was issued based on the increasing risks of cyberattacks in healthcare sectors. Indeed, attackers try to gain access to healthcare systems, such as hospital networks, clinic networks, or labs, to steal medical records or make online services unavailable for doctors and patients. Once the system is compromised, attackers can exploit data confidentiality, integrity, and availability of the whole system.

979-8-3503-3559-0/23/$31.00 ©2023 IEEE

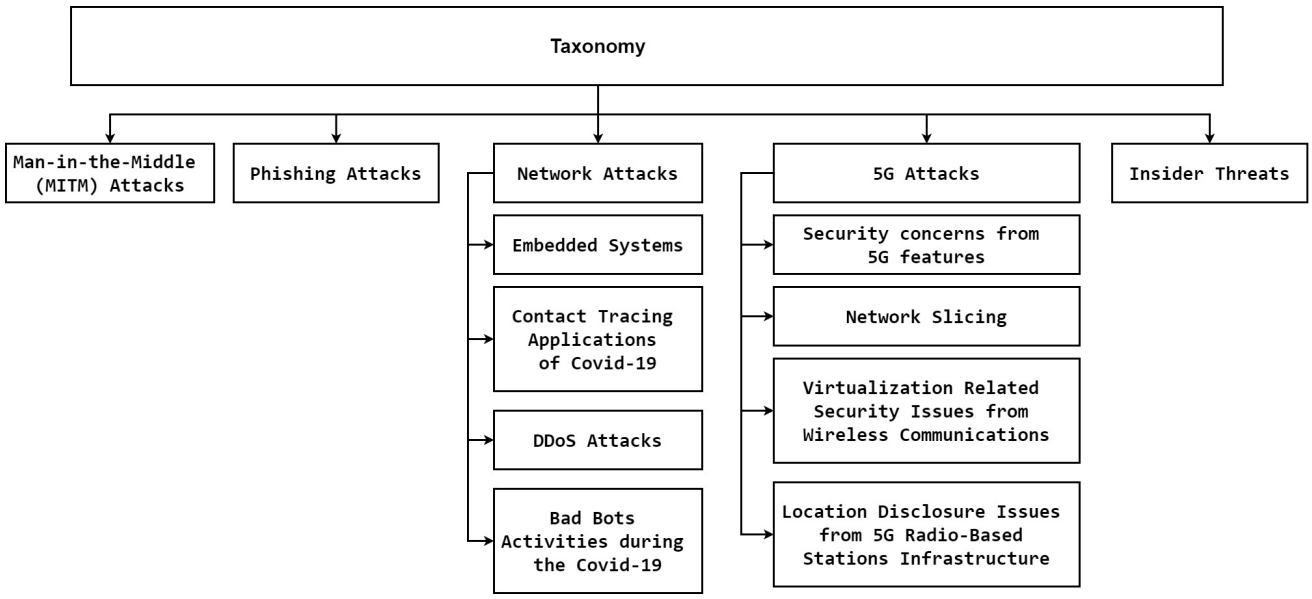

Fig. 1: Taxonomy of Major Threats during Covid-19 Pandemic

During Covid-19, healthcare organizations suffer various types of cyberattacks. Some existing attacks continue to increase with higher sophisticated levels. In this study, we focus on cyberattacks that significantly increase numbers compared to the reality before the pandemic. The following part discusses the current cyberattack situation in healthcare sectors and new techniques the attackers may use. We categorized the problem into five parts, Man-in-the-middle (MITM) attacks, phishing attacks, network attacks, 5G network attacks, and insider threats. Figure 1 demonstrates our taxonomy.

A. Man-in-the-Middle (MITM) Attacks

Man-in-the-middle (MITM) attack is one of the oldest forms of cyberattacks. Typically, a third person or a third party intercepts private communication between two end-users in this attack. Figure 2 shows an example case of MITM attacks. The ultimate goal of the MITM attack is to steal important personal information such as medical records, credit cards, or login credentials for different purposes. The attackers can use the stolen information for personal use, identity theft, or financial gaining.

Healthcare information is extremely sensitive compared to other records, making them more attractive to attackers. Healthcare record is one of the highest values in the black market with a mean price of $\$250$ per record. The next highest value record is payment card details which has a mean value of $\$5.40$ [22]. Communications between healthcare providers and patients were mainly conducted online during the Covid-19. The high demand for a secured network is evident for patients and doctors, especially those who reply on remote diagnosis and treatment. However, the current network used by several healthcare organizations places them in different potential MITM cyberattacks.

One of the new warnings from cybersecurity companies that help healthcare organizations inspect their networks is raising alarms for their internal cyber defense plans. Specifically, some healthcare organizations hire cybersecurity providers who use HTTPS interception products to detect malware in network traffic. However, the US Department of Health and Human Services (HHS) has shown cases in which HTTPS protocols could make the system more vulnerable to attackers [29]. One case given by the HHS is that HTTPS products of some cybersecurity providers do not check digital certificates in the chain of browsers. Every certificate contains a field called Certificate Authority (CA) flag that is set to ”true” if the public key being certified belongs to a CA and is ”false” otherwise. When the browser verifies a certificate chain of a domain, it checks that all certificates have the CA flag set to ”true” except for the leaf certificate for which the CA flag is skipped. Given that situation, if a browser does not check, no sender's identity verification will be implemented by a trusted authority in network communications. In addition, an attacker can use the certificate of a benign domain owned by the attacker (and signed by CA) to sign the attacker's malicious domain certificate. It means non-repudiation attacks may happen in

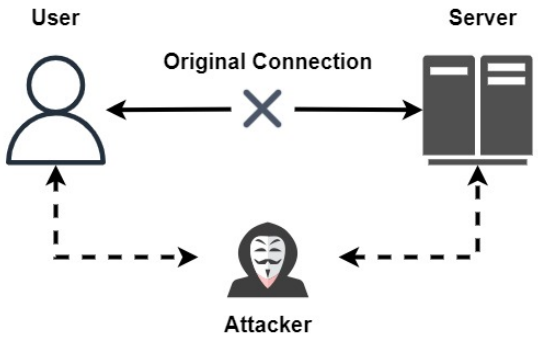

Fig. 2: Man-in-the-Middle Attack

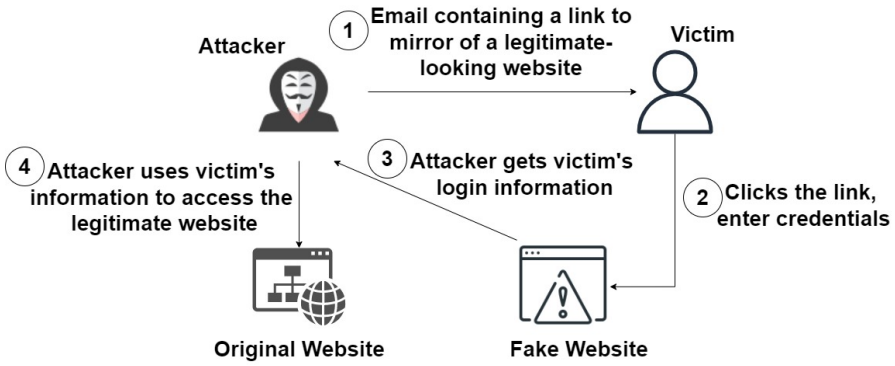

Fig. 3: Most Common Phishing Attack Scenario

this case. Man in the middle attackers pretend to be a trusted party that they are not. The case above points out that a regular security check from outside cybersecurity providers can create favorable conditions for attackers.

In another aspect, gaining access to the systems allows MITM attackers to implement different attacks on healthcare websites and applications. More people access healthcare websites to schedule testing, vaccine appointments, or read Covid-related news from those websites. Imperva report shows that there were more than 500 attacks per organization each month related to web applications in healthcare organizations in 2020 [24]. Cross-site scripting (XSS) attacks gained additional popularity during the Covid-19 pandemic, which targets all website users. During the XSS attack, malicious scripts are injected into a target website. When a user opens that website, the malicious code runs and allows the attacker to act like their victims to access other web sessions. IP, DNS, and HTTPS spoofing by MITM attackers can send victims to unbenign websites. Usually, users will not acknowledge that they are spoofed by a third person, so they keep sending all information they usually send. In this case, attackers can read all unencrypted data and control user interactions.

B. Phishing Attacks

Cybercriminals use phishing attacks to gain sensitive information from victims. Typically, attackers send a fraudulent message to trick the victim. Figure 3 shows the most common phishing attack scenario. In the figure, the attacker creates a mirror of the legitimate website and sends that fake link to the victim site. In case the victim clicks the link and provides login credentials, the attacker gets all the information and can use that information to access the victim's account on the legitimate website.

The recent outbreak of Covid-19 makes people spend more time going online to look for legitimate information from governments, trusted new agencies, or health organizations. The content analysis of Covid-19 themed phishing emails [2] pointed out some types of phishing attempts, including pretending to be WHO staffs to send out emails that provide information to prevent the spread of disease; offering fake financial benefits from governments such as Tax relief, stimulus checks, and cheap health insurances; offering a cure that is not approved by any health institutes in reality; asking for a donation to different funds and asking to do a survey with educational purposed. The demand for reliable sources for Covid-19 is getting higher day by day among people worldwide.

Besides phishing email, Smishing (SMS phishing) has become another popular platform that attackers use to spread malicious links and viruses. Millions of SMS messages containing viruses and malware are sent to millions of people every day without official warnings from government agencies. The common thing of scammers through SMS is that they will treat text receiver to click a link in the text messages to receive health test results, doctor's appointment, medicine prescription, free gifts, coupons, tax refund vouchers, parking decal refund, Covid-19 government assistance money, USPS deliveries, and shopping rewards. The increasing usage of the online platforms to log in to healthcare accounts during the Covid-19 leaves the attackers many opportunities to treat users to access their online accounts through not legitimate links. Hence, many users suffered from losing their sensitive information after the attacker exposed their usernames and passwords.

Phishing attacks during Covid-19 have some common themes. At the beginning of the pandemic, attackers focused on dynamic links that provided fake news about how dangerous the virus is to internet users. When the vaccine was available, the attackers immediately changed their themes to the Covid-19 vaccine and created new websites to host their phishing campaigns. According to a March 2021 report by Palo Alto Networks [26], tens of thousands of Covid-related spoof web domains were registered in one year since March 2020. One pattern for those websites is that internet users must fill out a Covid-19 Screening Form. The intruders attack the mental part of people who believe the screen form will be a passport for their traveling or working. Typically, the form will ask the users to put their emails and password. Ideologically, people usually use their real email passwords to put in the password field of the form. Consequently, the attackers collect emails and passwords that work for the same emails.

Vaccination verification created another vulnerability to cyberattackers. Many restaurants and public places only allow fully vaccinated people to get in. Some restaurants and public

places hire healthcare organization companies to provide online vaccination verification for their customers to save time. Taking advantage of that, attackers can send phishing emails with the name of some familiar healthcare organizations. In those phishing emails, recipients are prompted to fill out the form regarding two shots they already took, and they need to upload their vaccination card to a healthcare portal for verification purposes.

Phishing attacks keep emails as the primary method to lure legitimate users. However, the technique the attackers use is more sophisticated. Currently, several phishing attacks choose cloud-based platforms used for sharing files and information like Microsoft SharePoint, Google Drive, and Dropbox for their target. Instead of sending emails to healthcare staff, attackers simulate an automated message from one of the file-sharing platforms above, pretending to contain a document on the Covid-19 procedure. In most cases, the healthcare staff will not hesitate to click on those links at work since legitimate links come from a legitimate file-sharing platform. However, clicking the links will redirect the healthcare staff to a fake website hosted by Amazon Web Services (AWS). Another character in healthcare is prompting users (healthcare staff) to act immediately upon receiving documents from doctors or coworkers. The attackers can take advantage of that character to embed phishing emails with malicious links into current workflows.

C. Network-related attacks

Cybersecurity analysts reveal that healthcare organizations experience more significant risks than other organizations due to the complexity of the internet network, the diversity in embedded devices, and the expansion of manufacturer and type. Covid-19 puts several medical devices under the on-use mode regardless of days and nights. Some emerging issues that grab the attention of cybersecurity analysts are cyber-attacks on embedded systems, vulnerabilities from Covid-19 contact tracing apps, and DDoS attacks.

1) Embedded Systems

An embedded system is a microcontroller-based computing system to perform a dedicated task [11]. It can be an independent system or part of a more extensive system. One embedded system comprises hardware, software, and optionally mechanical parts. Thus, embedded systems refer to any computing subsystems other than general personal computers or mainframe computers [12].

Embedded systems have added social awareness to health data as an emerging field of the Internet of Medical Things (IoMT) has gained popularity. IoMT (also referred to as healthcare IoT) devices are internet-connected medical devices and applications which can connect to healthcare information technology systems. They can improve existing hardware such as electronic stethoscopes and imaging equipment, and we even see them being incorporated in commercial products such as smartwatches and phones. Moreover, IoMT helps doctors work with their patients remotely, making healthcare reachable to many whose mobility issues would have prevented such treatment. In addition, it enables real-time patient monitoring, which can increase diagnostic accuracy and urgent treatment cases. Securing these devices is vital because attacks on these devices can potentially cause life-threatening damage to the patients [31].

Software developers have to build the TCP/IP stack in which it is compatible with the features of the embedded devices. TCP/IP vulnerabilities allow attackers to use one single packet to crash or take control of those embedded devices. A recent study showed several new critical vulnerabilities in TCP/IP stacks, including uIP, PicoTCP, FNET, and Nut/Net [32]. Exploiting these vulnerabilities may allow attackers to gain access to the devices and remote code execution. Thousands of healthcare organizations around the world currently use those stacks. The internet function of most embedded devices nowadays is to provide more interfaces for internet users to communicate with those devices. That means the embedded devices become more open and easily accessible by outside users. The more features an embedded device has, the more chances an attacker can utilize to attack the device.

In another aspect, healthcare organizations may have hundreds of devices provided by several vendors. It takes time for each vendor to produce patches for vulnerable things. It also requires different procedures to use the patches from different vendors. The more diverse medical devices one organization has, the more vulnerable threats the organization faces.

2) Contact Tracing Applications of Covid-19

Contact-tracing apps are installed on smartphones that use Bluetooth signals to determine the distance between two users [3]. In case anyone has in contact with someone tested positive, the application notifies the user. In that case, the exposed user can get tested, self-quarantined, or mandatory-quarantined depending on the government rules. Many healthcare organizations and government agencies strongly suggest using contact tracing applications of Covid-19 to reduce the spread.

At first, this application brings positive feelings for people who crave a normal situation like the pre-pandemic era. However, the popularity of using the app poses different potential security risks related to data confidentiality. Disclosure of location becomes a significant problem for the app in case of a breach. Location is necessary for the app to do its job as a determinator that examines whether users have been in proximity. All users who use the app create a network of nodes where each user is considered a node. In case attackers gain access to the app server, they can form a social graph that makes users' contact profiles vulnerable.

Besides location disclosure issues, some possible attacks can be implemented to target various Covid-19 tracing applications, such as Bluesnarfing attacks, Replay attacks, and wireless device tracking. In Bluesnarfing attacks [33], adversaries connect to a Bluetooth-enabled device to access the device's resources without users acknowledging. Once the attacker has access to the device, sensitive information, such as personal photos, contact lists, emails, and passwords can be stolen. Replay attack is one of the lower-tier of Man-in-the-middle attack when an attacker who intercepts the data and

redirects them to their machine can trick legitimate users into receiving misleading contact data or sending their sensitive data to a compromised victim machine. Last but not least, wireless-device tracking utilizes various wireless technology such as WiFi, Bluetooth, GPS, and near-field communication [14]. With these technologies, adversaries can determine a user's location according to the tracking technology utilized. Wireless-device tracking, essential for contact tracing, is yet another feature that can be manipulated against app users. Attackers can access users' temporary IDs, device model information, and other personal information stored on the device. From identifiers in that harvested data, attackers can determine trends in where the users are and what activities they do, allowing them to exploit the user.

3) DDoS Attacks

With the spread of the Covid-19 virus over the last couple of years, the healthcare industry has been driving an urgent shift towards online services such as Telehealth and patient record access where a patient would discuss health issues over a Web/Mobile device camera session and be able to observe the results of a test or consultation. As a result, cybercriminals find it favorable to deploy denial of service (DoS) attacks targeting healthcare internet platforms.

The objective of a DoS attack is to exhaust the resources of a system until the system fails to provide its usual services in a timely fashion [1]. Typically, a DoS attack involves flooding a system by legitimate-looking traffic and making the system break down completely, work in less capacity, or fail to serve on time. A more severe type of DoS attack is distributed DoS (DDoS), where several compromised devices attack a victim simultaneously to amplify the attack. Deploying a DDoS attack does not require extensive knowledge since it can be purchased for as little as $5 per hour. This simplicity allows perpetrators to deploy attacks, and healthcare internet platforms are a good target because it affects many people. The following part discusses HTTP flood attacks, XML-based DDoS attacks, and BlackNurse - Black Storm attacks.

HTTP flood attacks: In an HTTP Flood attack, cybercriminals send an extensive amount of HTTP GET or POST requests to attack a web server or application. The packets are usually legitimate-looking; hence, it is arduous for the victim site defense mechanism to distinguish between attack and legitimate traffic. Eventually, the server gets overloaded and cannot accept requests or respond to intended users.

The most effective version of this type of attack is to force the server to allocate the maximum resources in each request. Therefore, HTTP-Post requests tend to be more effective from the attacker side. The main factor of the post message is sending the message body at a prolonged rate where the server needs to wait for the message to complete [15]. Because of the complexity of HTTP-Post, HTTP-Get based attacks are simpler and can be more effective in botnet DDoS attacks. Although HTTP Flood attack is not new, the cloud environment offers more chances through hyperconnectivity for attackers to implement this kind of attack with a more extensive scale of affected area and network.

XML-based DDoS attack (XDoS): The Simple Object Access Protocol (SOAP) is an XML-based protocol for exchanging structured information in web services. XDoS is another technique used by attackers to exhaust the system resources of the web services when the webserver processes SOAP messages. Traditionally, XDoS attacks use three strategies: oversized payload, external entity references, and entity expansion [4]. Cloud environment provides various web services like infrastructure or software as a service that helps the attackers implement XDoS attacks compared to the traditional physical setting.

BlackNurse and Black Storm attacks: The BlackNurse attack is a non-volumetric DoS attack type based on ICMP flooding that overloads web application firewalls [5]. It relays on ICMP Type 3 Code 3, "port unreachable" which is the usual answer returned on a UDP packet sent to a not-active port. Because of the many ICMP attacks, most ICMP packets are blocked on firewalls. However, some ICMP packets, including port unreachable, are necessary to allow the network to work properly.

More recently, a cybersecurity company NexusGuard introduced a new DDoS attack technique which is called Black Storm [6]. Black Storm attacks are similar to BlackNurse attacks, except they are employed in a reflective manner. Attackers generate spoofed UDP requests to the victim's closed UDP ports. The victim site devices respond to these requests as "port unreachable" messages. Finally, more devices continue to respond, the volume of responses completely overwhelms the target.

This attack has a massive capacity of occurrence on IoT medical devices because constrained application protocol specifically developed to support communication between those devices using UDP. Additionally, overwhelming IoT devices are relatively easier than high-end servers.

4) Bad Bots Activities during the Covid-19

Bad bots are another major pandemic desolating the Internet during the Covid-19 time. Some of the high-end bots have the ability to mimic human interactions in highly compelling ways, which makes it difficult to detect by defense mechanisms [8]. When more IoMT devices connect to the internet, they create a large attack surface for cybercriminals. Attackers can compromise nodes and turn them into bots. It is reported that the attackers have already compromised IoT devices to conduct large-scale DDoS attacks [7]. Therefore, protecting medical devices, especially wearable IoT devices, are crucial. According to the Imperva report in early March of 2021 [9], they have monitored a 372 percent spike in bot traffic globally on healthcare websites since September 2020.

In addition to the attack traffic on websites, scalping with bad bots created a significant issue during the pandemic. Scalping is buying high-demand products and reselling them at higher prices. Especially at the beginning of the pandemic, scalpers were deploying bots to buy extensive inventories of personal care products. As a result, most products were impossible to find in-store or online. In other healthcare aspects, a lousy bot can attack websites that people use to set up an

appointment for Covid testing or Covid vaccine. Data scraping is another activity that bad bots can implement. Bad bots may scrape any data related to vaccine availability, appointments, and inventory stocking that, in one way or another, may negatively affect healthcare sites. For example, bad bots may hold items in shopping carts, preventing healthcare customers from accessing pharmacies' websites.

Attackers also use bad bots to post comments and spread fake news on social media platforms. The emergence of social media bots put humans in a controlled environment where public opinion can be manipulated [10]. Bad bots can spread misinformation faster than humans. None will know whether the post about Covid-19 belongs to a bot; they only know the WHO or CDC organizations behind those posts. As a result, bad bots who pretend to be legitimate healthcare organizations can trick innocent people into accepting the false reality of the Covid-19 pandemic.

D. 5G Network Attacks

5G is the fifth-generation wireless cellular network to meet the dramatic increase of mobile devices used worldwide [16]. Followed by the rise in mobile devices, mobile data is also expected to grow extensively in the next decade. The 4G network will not be solid and fast enough to process future mobile data. Therefore, 5G network is designed to deal with a very high volume of data packets with a low tolerance for delay. The internet architecture also needs to be compatible with recent developments, especially appropriate for the 5G network [17]. Mobile data streaming is getting significant and changeable recently, so using 5G will support real-time access and quickly adapt to changes [16]. As the latest generation of mobile wireless technology, the 5G network provides users opportunities to experience a high-speed network, big capacity, and scalability.

The Covid-19 pandemic creates challenges in creating secure and reliable virtual access to healthcare websites and databases from mobile phones. Several services are on-demand by users. One physical station that stores all services to handle users' transactions may be overloaded. As a result, some healthcare organizations combine 5G network functions and cloud technologies to solve the limitations of the current frameworks [18]. In another aspect, the combination between 5G and cloud services poses some security concerns for cyber teams of several healthcare organizations. This subsection will discuss some core issues from the variety that may break the cyber defense framework of any system.

1) Security Concerns from 5G Features

One of the essential features of the 5G network is enhancing the communication between different internet-enabled devices on cloud infrastructure. The feature also raises a decentralized security concern. 4G network contains fewer connection points, making it easier to monitor, perform security checks, and upkeep the system. 5G technologies require more traffic routing points because of the shorter data transmission distance [19]. It means that telecommunication companies must spend more money and time monitoring and checking all those points because if one point gets compromised, it may affect other points-of-contacts and the whole system.

The Internet is decentralized, and provider companies are independent. There are many companies involved all around the world. Therefore, the transition from 5G from previous generation networks like 4G will take several years. Mobile operators that provide 5G need to support previous generations as well, which brings the earlier vulnerabilities from older generations, including SMS interception and geotracking [30].

Another security concern from 5G technologies is the improperly encrypted information of IoT devices. It provides attackers a convenient way to conduct their data triage procedure before any significant attacks. Knowing information about devices' operating systems helps attackers pick the right tool to implement their attacks. Once they have proper tools, the level of damage of those attacks will be more considerable. With such a substantial number of medical IoT devices operated at various hospitals and labs, the inconsistent security standards between those devices are inevitable. The inconsistency in security standards creates more possible breach points [19].

2) Network Slicing

Network slicing is an architecture to create multiple logical networks from a single physical network [20]. Mobile operators use network slicing to create virtual networks that focus on specific use cases to improve the quality of service. The tailored solutions from operators can increase the efficiency of their network, including providing high bandwidth solutions for video streaming and reducing the latency for online games. Dividing the network into isolated slices is a good security improvement since a comprised slice should not affect the other slices. However, this additional complexity brings more burden and careful implementation since the network operators need to deal with more complex network slides instead of a singular network. It is reported that incorrect configuration is the main reason for one out of three successful attacks on previous generation networks, including 4G [30]. Therefore, the additional complexity coming from increasing the number of slices on the 5G network may create additional vulnerabilities.

The idea of network slicing is not new, but it is now easily implemented under a 5G network with modern infrastructure and programming. Firstly, to advance the performances of individual slices, the network operators need to provide specific policies and standards of using separately and independently users' bandwidth. Cybercriminals can break borders between the network slices to stop the normal working of any users and reduce the network's resilience. In another aspect, unintentional behaviors or events created by legitimate users can affect the performances of other users' network slices. Secondly, authentication and encryption algorithms need baseline security for all users regardless of their purposes. Healthcare organizations use HIPAA to reflect their cybersecurity rules. However, HIPAA does not mention new baseline security with 5G technologies, which is still a big vulnerable hole for attackers to exploit. Thirdly, the heterogeny of medical data opens challenges of transmitting massive amounts of data with different types, datasets, and sizes. Finally, one

of the traditional attacks that last through mobile devices is location tracking attacks. Recently, cybersecurity analysts still see the increasing attack trend in 5G network slicing during Covid-19. Usually, one network function will request to use another to implement users' tasks. An authorization ticket will be provided for that request. However, there is sometimes no check whether the user identity belongs to the slice that requests the network function. Thus, attackers can take advantage of that ignorance to create a fake identity and intercept the network.

3) Virtualization Related Security Issues from Wireless Communications

The 5G network functions are conducted at Software Defined Networking (SDN) and Network Function Virtualization (NFV) [21]. The traditional model uses dedicated hardware devices such as routers and switches to control the network traffic, whereas SDNs control virtual networks via software. Compared to the traditional model, SDN architecture is more centralized, and a point of failure in the controller can affect the entire network. One of the main advantages of SDN is openness and programmable. On the contrary, they are also one of the biggest security concerns and increase the vulnerabilities. Moreover, SDN security and vulnerability research is still at the initial level compared to the traditional network architecture [34].

The distribution of credentials and access keys between functions creates additional vulnerability. Wireless communications in healthcare are also vulnerable to spoofing attacks where attackers inject forged messages with a fake identity [23]. Any failures of virtualized components can lead to new attack vectors. Taking advantage of vulnerabilities from 4G that do not get patched on time to support 5G, cybercriminals can intercept users' communication by injecting unbenign messages under a fake identity to trick servers that they are the legitimate ones. As a result, the attackers can get the same benefits as legitimate users, and then they can implement more sophisticated cyberattacks on the network.

4) Location Disclosure Issues from 5G Radio-Based Stations Infrastructure

5G requires more transmitters to cover the same area as current 4G networks. Therefore, 5G radio-based stations will be built at several places. The modern wireless network needs more 5G traffic routing points to guarantee high-speed internet connection and the necessary preparation for cellular network architecture. Nonetheless, radio-based stations pose threats to many mobile devices. Indeed, attackers can create malicious radio base stations to hit connected phones. The widespread attack is that the attackers can track phone users' location once they acquire old and new temporary network identifiers of victims' phones. Moreover, fake emergency alerts can be sent to the user when the attacker takes control of the paging channel.

E. Insider Threats from Employees and Vendors

A survey conducted by KnowBe4 and Osterman Research [25] reveals that most employees who join the survey feel confident about creating a secure password but lack knowledge about phishing and social engineer attacks through phone calls or emails. The survey also shows that 45% of respondents believe their IT departments are responsible for taking care of all cyberattacks from inside and outside. That means those employees have no sense of precautious using strange emails with attachments or links. Although phishing attacks are among the most popular attacks during Covid-19, 24% of the respondents cannot identify what the attacks look like and how to avoid them if they accidentally deal with an attack.

Even though many healthcare employees receive security awareness training once a year, business email compromises and phishing-related data breaches are pretty common in the healthcare sector. According to the U.S. Department of Health and Human Services Office for Civil Rights Breach Portal, there were 876 breaches within the last 24 months (from 02/27/2020 - 03/18/2022) [35]. It is reported that 267 of the attacks are related to email. It shows that $46,222,711$ out of $60,036,857$ people are affected by the breaches, which shows the significance of the problem.

Vendors who work with healthcare providers may access the same systems for their work purpose. It is not easy to manage all access points to sensitive information because it is a united system. Not many healthcare organizations have a comprehensive system to manage what medical devices are active and not involved. Thus, it is hard for organizations to measure any vulnerabilities in their medical devices. Consequently, they cannot list which devices should be updated, which ones should be patched or replaced by a new one with a new operating system. It is reported that 247 attacks out of 876 breaches occurred because of healthcare vendors, and $23,479,982$ people are affected by those breaches [35].

III. Conclusion

The coronavirus pandemic changed our day-to-day lives. The rate of Internet usage increased drastically, and exploiting vulnerabilities became more easier. During the pandemic, cybercriminal activities increased significantly, especially the healthcare sector was one of the top targets. In this paper, we review the significant cybersecurity problems in the healthcare industry during the Covid-19 era. It is crucial to understand possible threats, assess vulnerabilities, and take precautions to be ready for an attack.

References

[1] A. Y. Nur and M. E. Tozal, "Record Route IP traceback: Combating DoS Attacks and the Variants", Computers & Security, Vol. 72, pp. 13-25, 2018

[2] N. Akdemir and S. Yenal, "How Phishers Exploit the Coronavirus Pandemic: A Content Analysis of COVID-19 Themed Phishing Emails", SAGE Open, Vol. 11.3, 2021

[3] D. Lewis, "Contact-tracing Apps Help Reduce COVID Infections, Data Suggest", Nature, pp. 18-19, 2021

[4] X. Ye, "Countering DDoS and XDoS Attacks against Web Services", IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2008

[5] Erik Hjelmvik, BlackNurse Denial of Service Attack, Retrieved March 28, 2022, https://netresec.com/?b=16B68a3
[6] NexusGuard, A New Threat to CSP Networks – The Impending "Black Storm", Retrieved March 28, 2022, https://blog.nexusguard.com/white-paper/a-new-threat-to-csp-networks-the-impending-black-storm
[7] K. Angrishi, "Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets", ArXiv e-prints, arXiv:1702.03681, 2017
[8] X. Li, B. A. Azad, A. Rahmati, and N. Nikiforakis, "Good Bot, Bad Bot: Characterizing Automated Browsing Activity", IEEE Symposium on Security and Privacy, 2021
[9] Imperva Bad Bot Report 2021: The Pandemic of the Internet, Retrieved March 28, 2022, https://www.imperva.com/resources/resource-library/reports/bad-bot-report/
[10] M. Bondy, "Bad Bots", The Project on International Peace and Security, Institute for the Theory and Practice of International Relations, College of William and Mary, 2017
[11] D. Papp, Z. Ma and L. Buttyan, "Embedded Systems Security: Threats Vulnerabilities and Attack Taxonomy", 13th Annual Conference on Privacy, Security and Trust (PST), 2015
[12] A. Aloseel, H. He, C. Shaw, and M. A. Khan, "Analytical Review of Cybersecurity for Embedded Systems", IEEE Access, vol. 9, pp. 961-982, 2021
[13] B. L. Williams, "Information Security Policy Development for Compliance", CRC Press, 2013
[14] A. T. Kunnath, P. Preeja, and M. V. Ramesh, "ER-Track: A Wireless Device for Tracking and Monitoring Emergency Responders", Procedia Computer Science, vol. 10, pp. 1080-1085, 2012
[15] C. Easttom, "Network Defense and Countermeasures: Principles and Practices", Pearson IT Certification, 2013
[16] N. Hassan, K. L. A. Yau, and C. Wu, "Edge Computing in 5G: A Review", IEEE Access, vol. 7, pp. 127276-127289, 2019
[17] T. Hoeschele, C. Dietzel, D. Kopp, F. H. P. Fitzek, and M. Reisslein, "Importance of Internet Exchange Point (IXP) Infrastructure for 5G: Estimating the Impact of 5G Use Cases", Telecommunications Policy, vol. 45, 2021
[18] E. Skondras, A. Michalas, and D. D. Vergados, "Mobility Management on 5G Vehicular Cloud Computing Systems", Vehicular Communications, vol. 16, pp. 15-44, 2019
[19] Kaspersky, Is 5G Technology Dangerous? - Pros and Cons of 5G Network, Retrieved March 28, 2022, https://usa.kaspersky.com/resource-center/threats/5g-pros-and-cons
[20] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network Slicing in 5G: Survey and Challenges" IEEE Communications Magazine, vol. 55, pp. 94-100, 2017
[21] I. Ahmad, J. Suomalainen, and J. Huusko, "5G-Core Network Security", Wiley 5G Ref: The Essential 5G Reference Online, pp. 1-18, 2019
[22] Trustwave, The Value of Data, 2017, retrieved March 28 2022, https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/introducing-the-value-of-data-report/
[23] N. Wang, J. Tang, and K. Zeng, "Spoofing Attack Detection in Mm-Wave and Massive MIMO 5G Communication" IEEE Conference on Communications and Network Security (CNS), 2019
[24] Imperva, Volume of Web Application Attack, 2020, Retrieved March 28 2022, https://www.imperva.com/blog/web-application-attacks-on-healthcare-spike-51-as-covid-19-vaccines-are-introduced/
[25] KnowBe4, 2021 State Privacy and Security Awareness Report, Retrieved March 28 2022, https://www.knowbe4.com/hubfs/2021-State-of-Privacy-Security-Awareness-Report-Research_EN-US.pdf?hsLang=en-us
[26] Palo Alto Networks, 2021 Unit 42 Ransomware Threat Report, retrieved March 28 2022, https://www.paloaltonetworks.com/resources/research/unit42-ransomware-threat-report-2021
[27] Equifax Data Breach Settlement, retrieved March 28 2022, https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement
[28] Centers for Disease Control and Prevention, Health Insurance Portability and Accountability Act of 1996 (HIPAA), retrieved March 28 2022, https://www.cdc.gov/phlp/publications/topic/hipaa.html
[29] US Department of Health and Human Services (HHS), Man-in-the-Middle Attacks and HTTPS Inspection Products, retrieved March 28 2022, https://www.hhs.gov/sites/default/files/april-2017-ocr-cyber-awareness-newsletter.pdf
[30] 5G Security Issues, retrieved March 28 2022, https://www.gsma.com/membership/wp-content/uploads/2019/11/5G-Research_A4.pdf
[31] G. Thamilarasu, A. Odesile, and A. Hoang, "An Intrusion Detection System for Internet of Medical Things", IEEE Access, vol. 8, 2020
[32] Forescout Research Labs, How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices, retrieved March 28 2022, https://www.forescout.com/resources/amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices/
[33] A. J. Solon, M. J. Callaghan, J. Harkin, and T. M. McGinnity "Case Study on the Bluetooth Vulnerabilities in Mobile Devices", IJCSNS International Journal of Computer Science and Network Security, vol. 6, pp. 125-129, 2006
[34] B. Lin, X. Zhu, and Z. Ding, "Research on the Vulnerability of Software Defined Network", Advances in Engineering Research (AER), vol. 148, 2017
[35] U.S. Department of Health and Human Services Office for Civil Rights, Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, retrieved March 28 2022, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf