International Journal of Computer Techniques–IJCT Volume 12 Issue 6, November 2025
Open Access and Peer Review Journal ISSN 2394-2231 https://ijctjournal.org/

A Comparative Analysis of Various Cyber Attacks: Healthcare System

Prachi Verma
Information Technology & Computer Application Department
Madan Mohan Malaviya University of Technology
Gorakhpur, India
prachi.verma1499@gmail.com

Dr. Ganesh Chandra
Computer Science and Engineering Department
Madhav Institute of Science and Technology
Gwalior, India
ganesh.iiscgate@gmail.com

Abstract— *Healthcare industry plays an important role in everyone's life. Today, healthcare industry is fully depending on information technology as similar to other domains such as educational, research etc. As a result of technological advancement, healthcare industry opens the door for variety of cyber-attacks. In this paper we present the various types of cyber-attacks that are rapidly taking place in the healthcare industry and we also discuss about the most destructive cyber-attack (case studies) which taken place in healthcare domain and it was observed that due to these cyber-attack case studies, huge losses were suffered. In this paper we also tried to pay attention on the various possible key points which are helpful to keep save the healthcare industry from various cyber-attacks.*

Keywords— *Healthcare System, Cyber-attacks, Cyber Security.*

1. Introduction

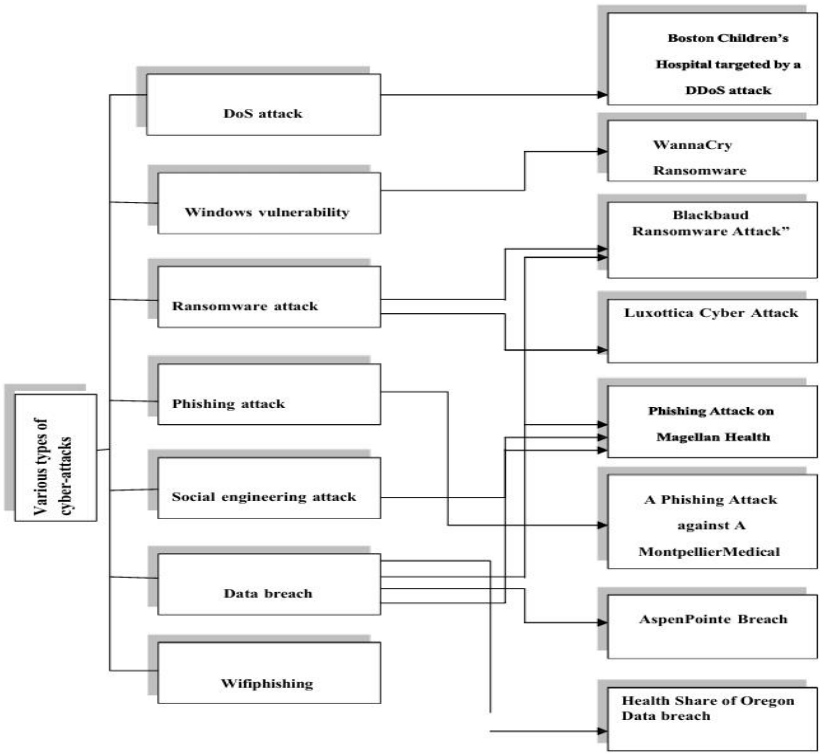
Cybersecurity attacks are costing medical care associations a large number of dollars every year. With the rapid development of medical technologies and clinical gadgets, medical care area is confronting digital protection issues. The medical care business has been likely the most intensely focused on initiatives throughout the course of recent years for various reasons, one of which is the pervasiveness of health information records in electronic form due to widespread digitization. [1][2].

The utilization of electronic patient information is unquestionably helpful for the clinical field since it has made it more straightforward to sort out, make due, and impart information instead of depending exclusively on looking through paper records to get information. The usage of electronic clinical benefits advancement has gotten sweeping across the clinical benefits industry and working on the organization of clinical consideration data and data is known. The key issue isn't the execution of clinical benefits advancement, but the shortfall of viable gamble the board systems to forestall cyberattacks.

Digital crooks designated different areas for assaults, yet medical care industry been designated not extremely lengthy after clinical consideration locale decided to rely upon the web to store information and make electronic structures. Clinical benefits information contains a great deal of data which can be used for a few unsatisfactory reasons by cybercriminals.

2. *Various types of Cyber attack*

Medical care industry experiences such countless kinds of digital assaults. There are different sorts of digital assaults that are rapidly goes in healthcare (as shown in figure1): DoS, Windows Vulnerability, Ransomware, Phishing, Social Engineering, Data breach and Wifiphishing.



a) DoS Attack

A Disavowal of-Administration (DoS) assault is an assault planned to shut down a machine or organization, making it hard to reach to its proposed clients. DoS attacks accomplish this by flooding the goal with traffic, or sending it information that sets off a mishap. In the two events, the DoS attack denies credible clients of the help or resource they expected. An additional kind of DoS attack is the Conveyed Forswearing of Administration (DDoS) attack. A DDoS attack happens when various structures sort out a synchronized DoS attack to a lone objective. The key differentiation is that instead of being attacked from one region, the goal is attacked from various regions on the double.

Specifically, DoS attack is a ruinous technique for attack which consumes the resources of a host or association until the system stops responding or crashes. In particular, DoS attack is a destructive attack which burns-through the assets of a distant host or organization until the framework quits reacting or crashes [3].

b) Windows Vulnerability

In setting of PC security, weakness is a shortcoming which can be manhandled by a risk performer (danger entertainer), like an attacker, to cross benefit limits inside a PC framework. Digital attack has turned into a critical concern throughout late years. While the particular capacity to attack has declined, hacking gadgets - both direct and expansive - are themselves progressing rapidly. Certain procedures are critical to safeguard a structure from computerized risks [4]. This work attracts with broad entry testing to find shortcomings in the Windows Server and try them. The window of weakness is the time from when the security opening was introduced or displayed in conveyed programming.

c) *Ransomware Attack*

Ransomware is a kind of malware that encrypts a casualty's records. The assailant by then demands a payoff(ransom) from the casualty to restore permission to the data upon portion [5]. Ransomware is a kind of harmful programming (malware) that does whatever it may take to circulate or ruins permission to data or a PC structure, by and large by encoding it, until the setback pays a result charge to the aggressor. When in doubt, the result demand goes with a deadline. In case the casualty doesn't pay on time, the data is away forever. Ransomware attacks are exceptionally ordinary these days. Huge associations in North America and Europe the equivalent have capitulated to it. Cybercriminals will attack any customer or any business and setbacks come from all endeavours [6].

d) *Phishing Attack*

Phishing is an association (network)type attack where the aggressor makes the fake (counterfeit) of an existing website page to trick an internet based client into motivate individual Data. Phishing is the mix of social planning and concentrated techniques to convince the client to reveal their own data [17]. Phishing is commonly finished by Email satirizing or messaging. It centres around the client who has no data about well-disposed planning attacks, and web security, like individuals who don't manage assurance of their records nuances like Facebook, Gmail, credit banks accounts and other money related records [7].

e) *Social engineering attack*

A social planning attack centers around this shortcoming by using different control procedures to bring out fragile information. The 'specialty' of influencing people to uncover delicate information is known as well disposed planning and the way toward doing known as a social planning attack is as well. There are various implications of social designing and different models of a social designing attack. Social designing attack detaches the attack into different classes and subclasses. The two classes of a social planning attack are: Immediate attack and circuitous attack. An immediate attack is an occurrence where no less than two people are locked in with a prompt conversation. This conversation can either be uneven or two-sided. Along these lines, this kind of attack is also organized into two unique approaches to bestowing: Bidirectional or unidirectional correspondence. Bidirectional correspondence is when no less than two social events take part in the conversation, toward the day's end, a two-way conversation occurs. Each get-together involves an individual, a social event of individuals or an affiliation. Unidirectional correspondence is a lopsided conversation where the social expert talks with the objective;however, the goal has no real way to convey back with the social designer. This is commonly finished through some correspondence medium, for instance, mass messages or short message organization (SMS). An indirect attack insinuates an event where an untouchable medium is used as a technique for conveying. Outcast mediums typically consolidate real mediums like blast drives, flyers or various mediums, for instance, site pages [8].

f) *Data Breach*

An information break is an occurrence where information is taken or taken from a framework without the data or endorsement of the framework's owner. A little association or gigantic association might persevere through a data enter (information break). Taken information might incorporate delicate, prohibitive, or confidential information, for instance, Mastercard numbers, client data, restrictive mysteries, or matters of public safety and wellbeing. The outcomes of an information break could incorporate mischief to the objective association's standing because of what is by all accounts "injustice of trust." On the off chance that connected records are fundamental for the data taken, casualties and their clients may likewise experience monetary misfortunes. [9].

g) *Wifiphishing*

Wifiphishing is a camouflaging assault procedure utilized on the Wi-Fi relationship to take critical data like login passwords, clinical record data, and so on. Wifiphishing incorporates two phases. The secondary stage includes a phony login page that is persuasively displayed on the client side, inciting the clients to enter the genuine affirmations to re-interface with the AP. The first stage uses a pernicious twin attack. In like way, the attacker can use any phishing pages to take basic information like patient doorway passwords. Wi-Fi Phishing is when digital

assaulter make a pernicious Wi-Fi passageway (access point) that seems comparative or indistinguishable from a genuine Wi-Fi passageway. This noxious Wi-Fi passageway is here and there known as the "evil twin" [10].

3. *Most destructive attacks of Healthcare*

a) *Blackbaud Ransomware Attack*

There is in every case a few events (good as well as bad) that stay in our memory until the end of time. Indeed, the digital assault of Blackbaud is without a doubt one of those event that will remain imprinted in our minds. A new report by DataBreaches.net predicts that the Blackbaud ransomware attack is viewed as most likely the greatest breaks of 2020 that incorporates patient health data (PHI), as

3.4 million patient records have now been represented as impacted [11]. It was in the long stretch of May that Blackbaud was tainted with a ransomware assault. Blackbaud, cloud programming provider, has been sued in 23 proposed purchaser class action cases in the U.S. likewise, Canada related to the ransomware attack and information enter. Notwithstanding the way that the association's network protection group had the choice to stop the attackers in mostly, the aggressors really had a good chunk of data with them like name, contact subtleties, wellbeing nuances, etc [12]. According to a Bleeping PC report, Blackbaud pronounced it had been named as a respondent in 23 putative client class movement cases: 17 in U.S. government courts, 4 in U.S. state courts and 2 in Canadian courts)[13]. Result of this assault is breaking the information of millions of patients; the aggressors actually had a decent lump of information with them like name, contact subtleties, wellbeing subtleties, and so forth [14].

b) *Luxottica Cyber Attack*

Luxottica, an eye-care conglomerate saw one of the most exceedingly awful cyber-attacks in the year August, 2020. Luxottica cyberattacks comes into the class of the major Ransomware assault. Luxottica, the world's biggest eyewear organization, has affirmed that it endured a ransomware assault which prompted the closure of its activities in Italy and China [15].

A Luxottica information break has revealed the individual and safeguarded wellbeing data information of 829,454 patients at Focal point Crafters, Target Optical, EyeMed, and other eye care practices. In a Security Episode, Luxottica uncovered that their course of action arranging application got through a data enter directly following being hacked. The uncovered information integrates individual data (PII) and safeguarded wellbeing data (PHI), including sicknesses and history [16].

c) *AspenPointe Breach*

This digital assault came into light in the month of September, 2020 in the Colorado Springs, Colorado, United States. AspenPointe, a behavioral and mental health provider, given an articulation saying that roughly the information of around 3 lakh patients was undermined. It was during this period that the organization needed to stop a majority of its operations for various days. An intensive investigation concerning this matter at long last could uncover that the programmers who were engaged with this assault had assembled data like contact subtleties, bank account details, date of birth, and so on [12].

d) *Phishing Attack on Magellan Health*

Scottsdale, Arizona witnessed a ransomware assault on Magellan Health Plan employees in April 2020. The severity of this attack led to 3.65 lakh patients and workers being affected. Five days before to the incident, hackers had successfully carried out a social engineering phishing attempt to acquire access by pretending to be a Magellan Health client [12]. Both employee and patient data, including login credentials and passwords, as well as data related to health insurance accounts, contact information, and other data, were taken.

e) *A Phishing Attack Against A Montpellier Medical Centre*

Phishing is the most expansive advanced danger, as demonstrated by the Corporate Digital protection Gauge circulated by the CESIN. A specialist of the Montpellier school clinical center found this out the most potential troublesome way in Walk, 2019 in Bristol, Joined Realm. Email contains an infection, more than 600 PCs perseveres around then, at that point. Fortunately, the clinic was using free inner organizations, which held the disease back from spreading to the sum of its 6,000 machines [18].

f) WannaCry Ransomware

WannaCry is a ransomware worm that spread rapidly through across different PC networks in May of 2017. Resulting to sullying Windows laptops, it scrambles reports on the PC's hard drive, making them unthinkable for clients to get to, and subsequently demands a payoff installment portion in digit coin to decode them [19].

The NHS in the UK was the target of the WannaCry cyberattacks, which infected more than 200000 PCs in 150 countries. By exploiting Windows vulnerability, the hackers were able to compromise 16 hospitals and 200,000 PCs, causing the cancellation of over 1,200 pieces of diagnostic equipment and approximately 20,000 appointments [18].

g) Boston Children's Hospital targeted by a DDoS attack"

2014 saw the first DDoS strikes by a hacktivist organisation targeted against a medical institution, Boston Youngsters' Clinic. Since the crisis center offers a Network access Supplier (ISP) with seven other close by medical care offices, the planned DDoS assaults could cut down various pieces of Boston's essential clinical consideration framework [16], [21].The medical clinic, whose gifts page was closed somewhere around the assault, is assessed to have lost 300,000 dollars on fixes to its computer systems [12].

h) Health Share of Oregon Data breach

What could be more awful than breaching information by stealing a laptop that had information of not hundreds, not thousands but rather lakh of individuals? This is exactly what happened when the laptop possessed by a transportation vendor of the Health Share of Oregon got taken and information of about 6.5 lakh patients was in question [20].

The laptop that got stolen had data about the contact subtleties of the patients, Medicaid ID numbers, date of birth, and so on. The lone thing that soothed the strain somewhat was that the gadget had no data about the health history of the patients [12].

The important information related to attack is shown in table 1, This chart details the multiple devastating attacks that have already occurred in the healthcare sector and the terrible effects of those attacks. In addition to these assault case studies and information about their global location and year of occurrence, this table also includes information about the types of attacks that have been utilized in the past. It also demonstrates the effects of these assaults.

4. Important information about Attacks Case Studies

S.No.	Name of Attack	Year	Location	Methodology behind the Attack	Impacts of the Attack
1.	"The Blackbaud Ransomware Attack"	May,2020	U.S and Canada	Ransomware assaults and information break.	Breaching the data of millions of patients, the attackers still had a good chunk of data with them such as name, contact details, health details, etc.
2.	"Luxottica cyber attack"	August, 2020	Italy and China	Major ransomware attack	It was found that the data about prescriptions, health insurance details, date and time of appointment, credit card information, etc. of as many as 829,454 lakh patients were stolen.
3.	"AspenPointe Breach"	September, 2020	Colora do Springs , Colora do, United states	Data breach	Stole large amount (295,617patients) of data that included patients' personal and healthcare information.

4.	"Phishing Attack on Magellan Health"	April, 2020	Scottsdale, Arizona, United States	Social engineering attack data breach by phishing attack	The aggressor elated delicate information, for example, names, contact data, representative ID numbers, federal retirement aide numbers and citizen distinguishing proof numbers
5.	"A phishing attack against a Montpellier medical centre"	March, 2019	Bristol, United kingdom	Widespread cyber threat phishing attack	Infect more than 600 computers to just open an e-mail which containing virus
6.	"WannaCry ransomware"	May,2017	Worldwide	Windows Vulnerability	Infect more than 200000 computers across 150 countries.
7.	"Boston Children's Hospital targeted by a DDoS attack"	2014	Boston, USA	DDoS(Distributed denial of services)	Is assessed to have lost 300,000 bucks on fixes to its PC framework.
8.	"Health Share of Oregon Data breach"	January, 2020	Clackamas, Multnomah, or Washington counties	Data Breach	Stolen data of about 6.5 lakh patients such as contact details of the patients, Medicaid ID numbers, date of birth, etc.

5. Discussion & Conclusion

A definitive objective for medical care suppliers is to give quality medical care administrations by using medical care innovation; in the event that network safety techniques are not as expected executed, then medical care associations should put away more cash managing digital breaks. With additional clinical gadgets becoming web associated and information being moved in an electronic structure, security disappointments are being perceived. The expansion in network protection isn't the way to addressing this issue; all things being equal, wellbeing leaders need to sort out some way to execute network safety practices and medical care consistence, for example, using review controls.

Current medical care is profoundly interlaced with innovation. From the complicated machines used for diagnosing contamination to the endeavor undertaking frameworks that store patient records, it's extremely difficult to run any clinical consideration affiliation today without seriously relying upon information advancement. In any case, similarly as with each and every other industry, the chances that accompany IT are not without their dangers—the greatest of these dangers is network safety dangers. Information defilement, unapproved framework access and malware contamination, are a portion of the things you need to monitor as a medical care IT or medical services the board proficient. The accompanying tips are fundamental in raising your medical services frameworks' network protection to an acceptable level [22].

- *Network protection Preparing for Staff*
- *Apply Programming Updates Expeditiously*
- *Execute currently demonstrated network safety advancements*
- *Controlled Framework Access*
- *Beat the Utilization of One Secret key for All Frameworks down*
- *Regular Risk Assessment*
- *Security Inside and out*

- *Data Recovery*
- *Protect Mobile Gadgets*

If the rate of cyber-attacks are not decreases in the healthcare domain it becomes the destructive face of thedigitalized healthcare system. There is need to involve some cyber expertise in the healthcare domain which are able to deal with that particular type of security risk and find out the safest way to deal with problem.

Refrences

[1] Cabrera, E. (2016). Health Care: Cyberattacks and How to Fight Back. *Journal of Health Care Compliance.*

[2] Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we?. Bmj, 358.

[3] Li, F., Yan, X., Xie, Y., Sang, Z., & Yuan, X. (2019, October). A Review of Cyber-Attack Methods in Cyber-Physical Power System. In 2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP) (pp. 1335- 1339). IEEE.

[4] Stiawan, D., Idris, M. Y. B., Abdullah, A. H., AlQurashi, M., &Budiarto, R. (2016). Penetration Testing and Mitigation of Vulnerabilities Windows Server. IJ Network Security, 18(3), 501-513.

[5] Slayton, T. B. (2018). Ransomware: The virus attacking the healthcare industry. Journal of Legal Medicine, 38(2), 287-311.

[6] Ransomware attack definition Retrieved March 07,2021, from<https://www.proofpoint.com/us/threat-reference/ransomware>

[7] Gupta, S., Singhal, A., & Kapoor, A. (2016, April). A literature survey on social engineering attacks: Phishing attack. In *2016 international conference on computing, communication and automation (ICCCA)* (pp. 537-540). IEEE.

[8] Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014, August). Social engineering attack framework. In *2014 Information Security for South Africa* (pp. 1-9). IEEE.

[9] Data breachRetrieved March 09,2021, from<https://www.trendmicro.com/vinfo/us/security/definition/data-breach>

[10] Sethuraman, S. C., Vijayakumar, V., & Walczak, S. (2020). Cyber-attacks on healthcare devices using unmanned aerial vehicles. *Journal of medical systems*, *44*(1), 1-10.

[11] Chernyshev, M., Zeadally, S., &Baig, Z. (2019). Healthcare data breaches: Implications for digital forensic readiness. Journal of medical systems, 43(1), 1-12.

[12] About cyber-attacks in healthcare industry. Retrieved April 10, 2021 from <https://www.analyticsinsight.net/top-4- cyberattacks-that-shook-the-healthcare-industry-in-2020/>

[13] Blackbaud sued after ransomware attack. Retrieved April 10, 2021 from< https://www.securitymagazine.com/articles/93857- blackbaud-sued-after-ransomware-attack >

[14] Healthcare data breach report. Retrieved April 10, 2021 from <ci.security/resources/news/article/recent-spike-in-healthcare- breach-reports-due-to-blackbaud-ransomware-attack>

[15] Luxotticacyber attack. Retrieved April 10,2021 from <https://www.insurancebusinessmag.com/asia/news/cyber/eyewear- giant-gets-blindsided-by-cyberattack-234390.aspx>

[16] Chen, Y., Dong, F., & Chen, H. (2016). Business process and information security: A cross-listing perspective. Journal of Industrial Integration and Management, 1(02), 1650009.

[17] Gupta, S., Singhal, A., & Kapoor, A. (2016, April). A literature survey on social engineering attacks: Phishing attack. In 2016 international conference on computing, communication and automation (ICCCA) (pp. 537-540). IEEE.

[18] Attacks in healthcare industry, Retrieved may 06, 2021 from <https://www.provisiontech.in/top-5-cyberattacks-against-the-health-care- industry/>

[19] Wannacry ransomware. Retrieved april 19, 2021 from <https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how- does-it-infect-and-who-was-responsible.html>

[20] Health share of Oregon data breach. Retrieved may 06,2021from<https://www.zdnet.com/article/health-share-of-oregon-discloses-data- breach-theft-of-member-pii/>