Mitigating Security Threats in the Sharing of Medical Data: A Comprehensive Review

Submitted: 25 February 2025
Reviewed: 26 April 2025
Revised: 9 May 2025
Accepted: 13 May 2025

Akhil Sekharan[*]
https://orcid.org/0009-0002-1423-1830
Joby P.P.[**]
https://orcid.org/0000-0002-7414-1506
Praseetha V.M.[***]
https://orcid.org/0000-0003-2892-0004

Article submitted to peer blind review

DOI: https://doi.org/10.26512/lstr.v17i2.57418

Abstract

[Purpose] The medical field is one of the most regular targets of cybersecurity assaults, which occur extensively worldwide. Medical data security is of extreme importance. Medical data, often stored electronically, faces frequent attacks from both internal and external sources during transmission and storage. Data breaches are an important concern in the healthcare industry. Attackers may target medical data for financial gain or identity theft. Even a single breach can expose sensitive patient information.

[Methodology/approach/design] Cybersecurity measures are critical for safeguarding patient information and maintaining the integrity of healthcare applications in an increasingly digital healthcare landscape.

[Findings] Legal software systems with updated software are essential, along with ensuring that the medical data is only accessible to authorised persons.

[Practical implications] This paper explores the areas of cybersecurity relevant to healthcare applications, emphasizing the risks posed by well-known threats such as WannaCry, Medjack, NotPetya, and brainjacking.

Keywords: Cybersecurity. Medical data. Healthcare applications. Data breaches. Ransomware.

[*] Research Scholar at APJ Abdul Kalam Technological University, Thiruvananthapuram, India. Address: Department of Computer Science and Engineering, St. Joseph's College of Engineering and Technology, Palai (Autonomous), Choondacherry Post – 686579, Kerala. E-mail: akhilsekharan@gmail.com.

[**] Professor, Department of Computer Science and Engineering at St. Joseph's College of Engineering and Technology, Palai. E-mail: jobymone@gmail.com.

[***] Professor, Department of Computer Science and Engineering at St. Joseph's College of Engineering and Technology, Palai. E-mail: praseethasunil@gmail.com.

SEKHARAN, A.; P.P., JOBY; V.M., PRASEETHA. *Mitigating Security Threats in the Sharing of Medical Data: A Comprehensive Review*. **The Law, State and Telecommunications Review**, v. 17, no. 2, p. 134-151, October 2025.

INTRODUCTION

One of the crucial records that must be securely maintained is medical information, which is increasingly targeted by individuals worldwide seeking financial gain and engaging in other unethical activities. The transition from paper to electronic patient records has improved data integrity and security, ensuring access is granted solely to legitimate medical centers.

Despite these advantages, information in electronic media, like publicly displayed information with restricted access, can be exploited by those who gain access, whether legally or illegally. Such actions can compromise the data's integrity or even harm the public directly. Medical data shares similarities with this scenario. Unauthorized access to electronically stored medical data can have severe repercussions for the public.

Security incidents have affected numerous healthcare organizations worldwide that manage electronic medical data. Various methods can be used to breach the system or launch security attacks on the medical data (HOCKEY e A., 2020). Since the data is stored somewhat like a public platform, malicious individuals worldwide have increased opportunities to access it. Attackers may employ malware, insider assistance, or other means to target the system, whether overtly or covertly.

Medical centers serve as crucial repositories of patient data, using it to aid patients by considering their medical histories. We understand the extreme sensitivity of medical information and how challenging it is to safeguard it from external parties. Consequently, fraudsters are inclined to attack and steal this sensitive data.

In certain situations, such as during pandemics, government organizations themselves may retain medical information, including epidemiological data and patient medical conditions. Even the storage of medical data poses security risks, and the exchange of such data introduces new vulnerabilities.

People are particularly concerned about medical data, fearing the misuse of their personal information or the exposure of their medical history to strangers. The UK's healthcare organizations have faced numerous cybersecurity attacks, with nearly half of the security issues resulting from malware or virus attacks. Outsiders may gain access with the assistance of insiders, such as organization employees. The absence of standards and norms, along with the habit of clicking on hazardous links, contributes to these security breaches.

BACKGROUND WORK

This paper attempts to address numerous security issues related to both the storage and exchange of medical data while also conducting a comparative analysis of existing methods aimed at preventing security breaches.

THREATS AND SECURITY

Medical records must be kept electronically on a physical device or in the cloud. Healthcare practises need to take every precaution to improve healthcare data security and stop hackers from compromising their data, as ransomware is on the increase and cyber attackers are becoming more self-assured and aggressive in their attacks.

Sometimes, information needs to be transferred from one source to another, or stakeholders may want to access the data directly from the source. The reasons for security breaches and the necessity of security are now evident. Medical data transfer can be vulnerable to attacks by external parties, whether the data is encrypted or transmitted in its unaltered form. These attacks can be passive or aggressive.

Over 70% of data breaches occur in the medical industry, with various attack types, including malicious hacking, insider assaults, Physical harm, including loss or theft of paper data and loss or theft of portable electronic devices (SEH et al., 2020). Approximately 60% of these attacks involve hacking or the deployment of malicious software. Data infringement results in financial losses, harm to reputation, and decreased safety of patients. According to reports, the medical card numbers of every Australian citizen are available for sale on the dark web (P. et al., 2017).

While encrypted data is generally challenging to decrypt, the choice of encryption technique is crucial. Any security system can be breached by someone using incredibly powerful machinery. Sometimes, the encryption methods we employ may not be suitable for the situation. For example, Convolutional Neural Networks (CNNs) are a sort of deep learning neural network that are particularly effective in processing and analyzing visual data. CNN algorithms in secure IoT healthcare applications can enhance the accuracy, efficiency, and security of data processing, analysis, and decision-making, contributing to improved patient care and data protection. But the cost and implementation time may hinder the successful use of the CNN algorithm in healthcare application (THILAGAM et al., 2022). The amount of data encrypted can be a concern when using the Advanced Encryption Algorithm (AES algorithm) in a cancer prediction system (ANURADHA et al., 2021). If the data size exceeds 300 KB, the key size becomes an issue in Lionized remora optimization (LRO) based encryption systems (ALMALAWI et al., 2023). The medical field has been targeted by WannaCry, Medjack, various types of brainjacking attacks, and other ransomware attacks (L.EVENSTAD et al., 2016; D. et al., 2015;L. et al., 2016).

WannaCry attack

According to Mohurle, S. et al. (MOHURLE et al., 2017), the WannaCry Ransomware Attack of 2017 was one of the most severe cyberattacks to date. WannaCry is a malicious program that encrypts files or computer systems, preventing users from accessing them. It seizes ownership of the files or devices by demanding a ransom from the victim in exchange for a decryption key, which is required to regain access to the encrypted data or systems. Visualizing this situation can be challenging. The authors of the study concluded that the ransomware primarily spreads through phishing emails and visits to websites containing harmful software. Therefore, it is imperative for computer users to regularly back up their data.

The WannaCry cyberattack impacted approximately 230,000 computers globally, affecting a wide range of entities, including universities, corporations, government agencies, and more (Kaspersky, 2023; WIKIPEDIA, 2023; NDTV,2017; Staff, R. et al.,2017); Jones et al.,2017).

In the healthcare industry, particularly during the WannaCry attack, one of its most prominent targets was the National Health Service (NHS) in the United Kingdom. The WannaCry attack had a significant impact, affecting at least one-third of healthcare trusts throughout England (NATIONAL, 2017). Fig 1 shows the effect of wannacry attack on NHS, UK.

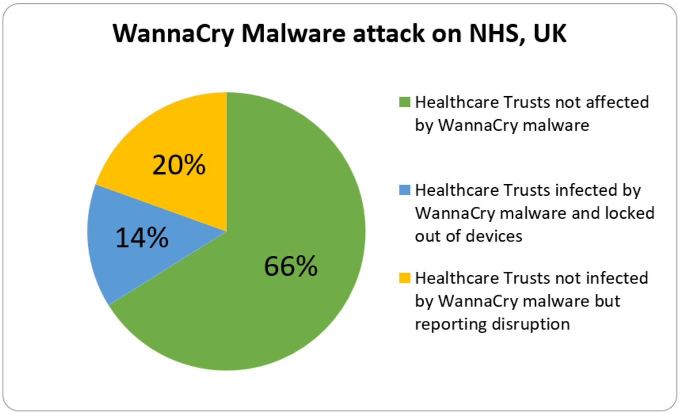


Fig1: Effects of WannaCry attack on NHS, UK

During the initial infection phase, WannaCry exploits the EternalBlue and DoublePulsar vulnerabilities, which were reportedly disclosed in 2017 by a group known as The Shadow Brokers (Akbanov et al. ,2018,2019a,2019b). EternalBlue targets a vulnerability in the server message block (SMB) protocol, which Microsoft had subsequently addressed (Betafred et al., 2017). This vulnerability allows attackers to implement a remote code on compromised machines by sending dedicated messages to an SMBv1 server, connecting to TCP ports 139 and 445 on Windows systems that haven't received security patches. Specifically, this vulnerability affects the majority of Windows operating system versions for which no security fix is available.

On previously compromised systems, DoublePulsar serves as a persistent entry point that grants access and allows program execution. With this capability, attackers can introduce additional software into the compromised machine. The WannaCry worm employs EternalBlue during the dissemination phase to initiate the initial infection by actively scanning the appropriate TCP ports for the SMB vulnerability. The DoublePulsar backdoor is then attempted to be implanted onto the compromised systems, if successful (Akbanov et al. ,2018,2019a,2019b). Without the user's involvement, DoublePulsar essentially provides hackers with control over the system, enabling them to install any malicious software of their choice (KOUJALAGI et al., 2018).

Medjack attack

A cybersecurity company called TrapX released a report describing three real hospital intrusions. These incidents exploited a vulnerability known as *Medjack*, short for medical device hijack. The researchers emphasized that when combined with this attack vector, medical equipment could be the most vulnerable point within a hospital's security infrastructure. They warned that *medjack* posed a significant threat to large healthcare institutions worldwide (STORM, 2015).

According to Alsubaei et al. (ALSUBAEI et al., 2019), in 2017, nearly half of all ransomware attacks targeted the Internet of Medical Things (IoMT). Within IoMT environments, *medjack* 2 effectively executed ransomware attacks, resulting in the unauthorized extraction of data. In 2017, the largest ransomware incident on record infected over 200,000 devices worldwide. Devices such as diagnostic tools (including CT scanners, PET scanners, and MRI Scanning machines), infusion pumps, medical lasers, surgical machines and other therapeutic equipment, life-sustaining devices (including heart/lung machines, medical ventilators, extracorporeal membrane oxygenation machines, and dialysis machines) are all vulnerable to *Medjack* (M. et al., 2016).

Medical devices used in hospitals and clinics must be regularly updated, and outdated equipment should be replaced to prevent potential security breaches.

Healthcare personnel, including nursing assistants, should exercise greater vigilance in managing and maintaining these devices to minimize the risk of security vulnerabilities.

Steps in Medjack attacking

The following steps can be used by an attacker to carry out a Medjack assault (MEGGITT e SINCLAIR., 2018):

Stage 1: The attacker selects a target after conducting research on the facility, then launches the assault to compromise at least one device.

Stage 2: The attacker successfully compromises the specific medical device using malware, establishing a covert access point into the network. They proceed to navigate the network, seeking to either steal data or infect other devices.

Stage 3: The attacker specifies the precise data they wish to steal, typically focusing on financial or medical details.

Stage 4: The attacker profits through various means, including identity theft, selling patient information on the black market, or employing ransomware, which encrypts data until the victimized company pays a ransom."

Fig 2 shows the different stages *in MedJack attack.*

Attacks like MEDJACK show the unpleasant fact that most hospitals are still ill-prepared to tackle these attacks. They are leaving themselves and their patients incredibly susceptible to damaging assaults by continuing to employ outdated medical technology and skimping on cyber protection. Attackers will keep taking advantage of this and develop increasingly complex attacks that are even more difficult to defend against. If hospital managers wish to avoid spending millions of dollars for attack cleanup, they can no longer bury their heads in the sand.

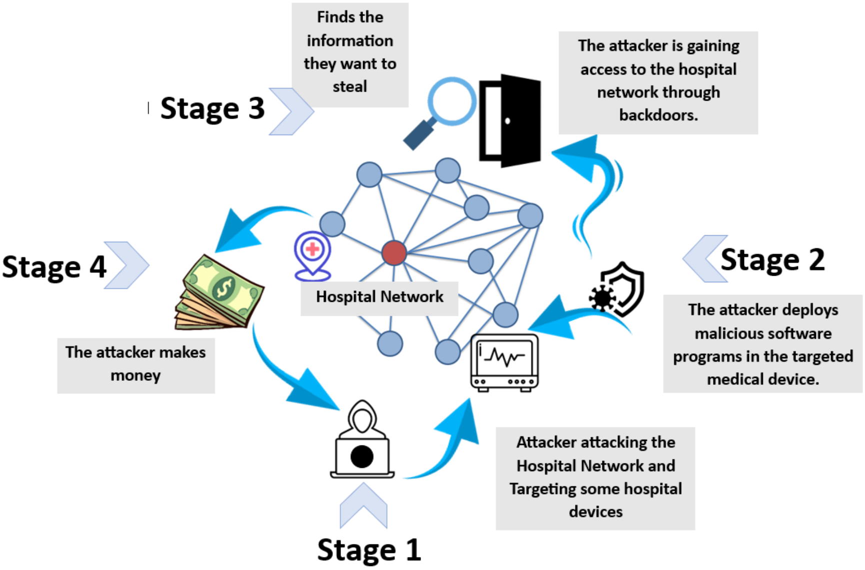
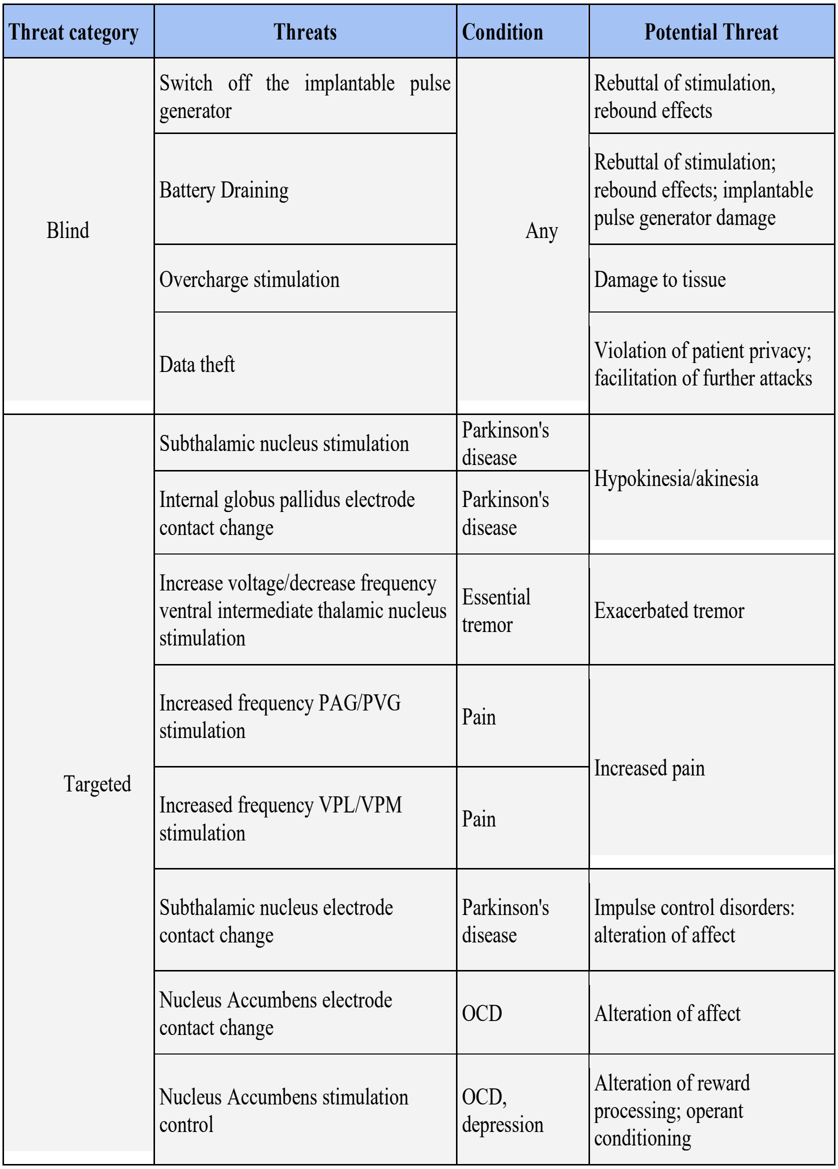

Stage 3
Finds the information they want to steal
The attacker is gaining access to the hospital network through backdoors.
Stage 4
Hospital Network
Stage 2
The attacker deploys malicious software programs in the targeted medical device.
The attacker makes money
Attacker attacking the Hospital Network and Targeting some hospital devices
Stage 1

Fig2: Different stages in MedJack attack

Brainjacking attack

In real-world brainjacking incidents, hackers target compromised medical devices. Through brainjacking, they gain unauthorized access to neural implants within an individual's body. Hacking into these brain implants could potentially grant the attacker control over the victim's cognitive and physical functions, resulting in serious consequences (Cisomag, 2022). There are several mechanisms through which attackers could manipulate patients if they gain unauthorized access to an implant. These mechanisms encompass blind attacks, where the attacker requires no patient-specific knowledge, and targeted attacks, which necessitate patient-specific information. Blind assaults can result in information theft, tissue injury, implant battery drain, and discontinuation of stimulation. Targeted assaults, on the other hand, can interfere with motor function, change impulse control, alter emotions or affect, cause pain, or disrupt the reward system. Table-1 shows the summary of various cyber threats in the network.



Threat category	Threats	Condition	Potential Threat
Blind	Switch off the implantable pulse generator	Any	Rebuttal of stimulation, rebound effects
	Battery Draining		Rebuttal of stimulation; rebound effects; implantable pulse generator damage
	Overcharge stimulation		Damage to tissue
	Data theft		Violation of patient privacy; facilitation of further attacks
Targeted	Subthalamic nucleus stimulation	Parkinson's disease	Hypokinesia/akinesia
	Internal globus pallidus electrode contact change	Parkinson's disease	
	Increase voltage/decrease frequency ventral intermediate thalamic nucleus stimulation	Essential tremor	Exacerbated tremor
	Increased frequency PAG/PVG stimulation	Pain	Increased pain
	Increased frequency VPL/VPM stimulation	Pain	
	Subthalamic nucleus electrode contact change	Parkinson's disease	Impulse control disorders: alteration of affect
	Nucleus Accumbens electrode contact change	OCD	Alteration of affect
	Nucleus Accumbens stimulation control	OCD, depression	Alteration of reward processing; operant conditioning

Abbreviations; OCD, obsessive-compulsive disorder; PAG/PVG, periaqueductal/periventricular grey matter; VPL/VPM, ventroposterior lateral/medial thalamic nucleus.

Table 1: Summary of Threats

Method of attack

An attacker has a number of tools at their disposal to control their victim's brain if they have managed to get past the device's protection. In order to regulate the strength of the stimulation, they can change the characteristics of the stimulus such as voltage or current, frequency, pulse width, and electrode contact (BUTSON et al., 2007). These possible assaults may not be fatal, but they nevertheless have the potential to cause great suffering. These assault tactics are extremely speculative and can need degrees of physical or informational access that are out of most attackers' grasp. However, it is crucial for clinicians to be on the lookout for these potential scenarios, especially as brain implants get more sophisticated and assault tactics become more varied and complicated(PYCROFT et al., 2016)

Brainjacking attacks can be categorized into two main types: blind attacks and targeted attacks. In blind attacks, the attacker doesn't focus on a specific patient, while in targeted attacks, a specific individual is the intended target. During a blind attack, the attacker typically lacks any extra information about the patient. The patient's specific condition could be unknown or could vary widely. In such cases, the attacker might deactivate the implanted pulse generator (IPG) device, thereby disrupting the patient's stimulation. Alternatively, they could cause significant harm by depleting the device's battery. In contrast, in a targeted assault, the attacker may possess some basic knowledge about the victim, such as the patient's current health status and physical condition (PYCROFT et al., 2016). Fig 3 shows the blind attack and targeted attack in brainjacking.

Brainjacking could directly endanger patients by allowing attackers to manipulate or disable critical neural implants, posing life-threatening risks. This would necessitate new clinical protocols to detect and respond to such attacks and could drive policy changes requiring stricter cybersecurity standards for implantable medical devices.

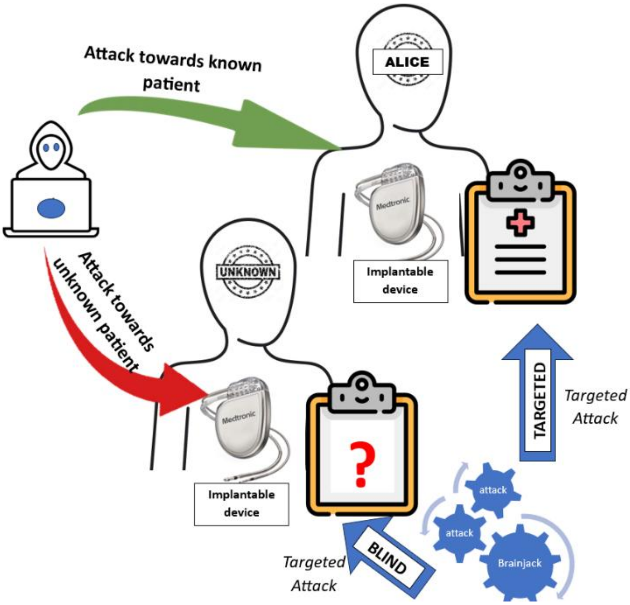


Fig 3: blind attack and targeted attack in brainjacking

NotPetya attack

The NotPetya malware, which bears a resemblance to the Petya ransomware, inflicted significant damage on several industries, including retail, transportation, advertising agencies, and law firms. This highly effective destructive program spreads across computers once it infiltrates a business network, systematically destroying the file systems of the affected workstations (Lika et al.,2018;I. et al.,2017).

Ukraine was the primary target of the NotPetya assault, which occurred on June 27, 2017, and immediately established itself as one of the most catastrophic cyberattacks in history. However, there was another aspect of the malware's impact that was difficult to measure: its effects on hospitals and the health of the medical personnel who worked there. One notable casualty of the NotPetya assault was the Ukrainian company Nuance. Hospitals comprised a significant portion of the company's business, as their doctors used Nuance's software to input updates to patient data, which was designed to automatically convert audio snippets into patient record updates. In fact, Nuance provided services to the majority of American hospitals, which felt the impact of this cyberattack on the healthcare industry (Greenberg, A. et al.,2019). Table 2 illustrates the Comparison of different attacks in medical domain.

Healthcare systems frequently face cyber threats, including hardware Trojans (T. Wehbe et al.,2017), Sybil attacks involving a single rogue node or a compromised IoMT (Internet of Medical Things) device (Ahmad et al., 2020), Denial of Service (DoS) attacks (Rashmi et al., 2015), and man-in-the-middle

(MITM) attacks (Vahab et al.,2012). These are in addition to the attacks already mentioned.

Attack Name	Year of 1st reported	Method of attack	Total estimated loss	Reference
WannaCry	2017	Exploit that makes use of a weakness in the SMB protocol for Windows	4 billion	(MOHURLE et al., 2017;Kaspersky, 2023;WIKIPEDIA, 2023;NDTV,2017;Staff, R. et al.,2017;Jones et al.,2017;NATIONAL, 2017;AKBANOV et al.,2018,2019;Betafred et al., 2017;KOUJALAGI et al., 2018;Berr, J. et al.,2017)
Medjack	2015	Breaching by using some malwares in medical device and attack	-	(STORM, 2015;ALSUBAEI et al., 2019;M. et al., 2016)
BrainJacking	2016	Breaching some implanted medical device and attack	-	(Cisomag., 2022;PYCROFT et al., 2016;BUTSON et al., 2007;CHAUDHURY e D., 2020)
NotPetya	2017	Exploit that makes use of a weakness in the SMB protocol for Windows	10 billion	(Lika et al.,2018;I. et al.,2017;Greenberg, A. et al.,2019)

Table 2: Comparison of different attacks in medical domain

RESULTS

The security of medical data is a significant concern for both patients and medical professionals. Achieving impenetrable security is unrealistic. WannaCry, Medjack, Brainjack, and the other mentioned assaults can occur regardless of the data storage which is local or the cloud. In addition to these threats, there are numerous other attacks in the medical field, increasing the risk during data transmission. Threats to medical data can manifest during transmission or storage. In response to these breaches in the medical field, we propose two approaches.

Implementation Approach

When overseeing medical data, it's essential to implement robust security measures and choose the most efficient method carefully. The choice of strategy depends on the specific situation.

For instance, consider a scenario where medical data is encrypted to safeguard against security concerns. These encryption algorithms play a vital role in protecting medical data from malicious intrusions. Encryption algorithms can be categorized into symmetric cipher and asymmetric cipher, based on keys (ABD et al., 2010;KARULE et al., 2016;HAMOUDA e B., 2020). Depending on the context, we have the flexibility to choose between symmetric and asymmetric encryption methods based on the feasibility of sharing encryption keys. In certain situations, steganographic techniques may also be considered to encrypt medical data by concealing it within various images, regardless of their relevance to the medical field.

However, it's worth noting that standard Algorithms like RSA, IDEA, DES, AES, and ECC, among others, are not suitable for real time image encryption due to their high computing time and processing power requirements (Laiphrakpam et al.,2017;Shankar et al, 2015).

Regarding the protection of medical data in the context of IoT, Thilagam, K. et al. (THILAGAM et al., 2022), have introduced IoT version of deep learning approaches focused on privacy protection. Their proposed model supports future smart healthcare systems, incorporating a privacy isolation zone and a cloud security model. While this approach enhances data transit and cloud-based storage security, it poses challenges in terms of time and cost (THILAGAM et al., 2022).

Additionally, Ali, Aitizaz et al. (Ali et al. ,2022) have developed a new deep-learning strategy-based safe searchable blockchain, enhancing user data access security. However, this system faces some limitations, particularly in terms of the loss function.

K. Shankar et al. (SHANKAR, 2018) have suggested a visual cryptography technique, which employs elliptical cryptography for visual cryptography to maintain image secrecy effectively. This approach offers exceptional performance but comes with increased time and cost requirements.

For addressing threats like WannaCry and Medjack, Akbanov et al. (Akbanov et al. ,2019b) have presented a strategy using Software-Defined Networking (SDN) for identifying and mitigating threats. This method focuses on monitoring DNS traffic to identify malicious domain names or IP addresses connected to WannaCry's Command and Control (C&C) server, effectively stopping any suspicious activity.

To effectively identify and handle ransomware threats like WannaCry and Medjack, Celiktas et al. (ÇELİKTAŞ, Barış., 2018) propose a ransomware detection and prevention system. This tool employs a dual-phase detection technique, simultaneously using a hybrid signature-based detection method and a hybrid anomaly-based detection method to analyze network connections and files for potentially harmful information.

Haque, Nur Imtiazul, et al. (HAQUE et al., 2021), describe the SMChecker system, a threat analysis model that addresses potential attacks on smart healthcare systems. This model uses machine learning to detect anomalies in sensor data and offers flexibility in decision-making. However, it also faces challenges related to time and cost.

Regarding brainjacking attacks on medical devices, such as insulin pumps, Rathore, H. et al. (RATHORE et al., 2017,2018) have developed neural network and deep-learning technologies to counteract fake glucose measurements in vulnerable devices, achieving high accuracy rates.

Finally, it's worth noting that with the emergence of quantum computing, ciphers that were once considered impenetrable, such as RSA and ECC, can now be easily cracked (KIRSCH et al., 2015).

Behavioral Approach

Diverse individuals interact with medical data on various occasions, including patients, healthcare professionals, government authorities, and support staff. How they handle this data is of immense importance, even if they may not always fully comprehend its significance, potentially creating vulnerabilities. Responsible individuals must oversee sensitive data management, which is a standard protocol aimed at ensuring data accuracy and security. As previously mentioned, medical information ranks among the most sensitive and frequently targeted by malicious actors. The National Cyber Security Centre provides a set of 10 recommendations for enhancing online security, which apply equally when dealing with medical data (N.C.S. e 10, 2016). Those entrusted with medical data should be well-informed about its importance and sensitivity, with other responsible authorities providing necessary guidance. Furthermore, it is essential to outline a foundational strategy for mitigating risks in challenging situations.

Software for medical devices often combines elements from third-party software vendors with specially designed code. While software developers can follow coding best practices to enhance the security of their unique code, vulnerabilities may still arise when third-party software components change over time (JUMP et al., 2019). Employees, including technical assistants and system administrators, should take the necessary precautions to prevent vulnerabilities caused by outdated or questionable software.

CONCLUSION

Protecting healthcare data during a time of digital transformation is a challenging and critical task. The healthcare industry is often targeted by cyberattacks, and data breaches can have catastrophic consequences. This study highlights the multifaceted nature of healthcare data security and addresses notable hacks and vulnerabilities within the industry.

The study proposes two approaches to enhance healthcare data security: a behavioral approach that emphasizes ethical data management and an implementation approach that focuses on encryption techniques. By adopting these methods, healthcare organizations can fortify their security measures, ensuring the integrity and confidentiality of patient data.

We will look into these strategies in more detail in the sections that come next, offering healthcare stakeholders insights and suggestions on how to reduce risks and guarantee the security of patient data. The healthcare industry can traverse the changing environment of cybersecurity threats and provide safer and more secure healthcare services by combining innovative technology and ethical behaviour.

Given the rapidly evolving threat landscape, future research should focus on securing emerging technologies like AI-powered diagnostic tools and IoT-based medical devices. There is also a critical need for the development of post-quantum encryption methods and real-time breach detection systems tailored to the healthcare ecosystem. Addressing these areas will be essential to staying ahead of sophisticated cyber threats in the coming years.

REFERENCES

Abd Elminaam, D., Abdual Kader, H.M. and Hadhoud, M.M. (2010) Evaluation of the Performance of Symmetric Encryption Algorithms. International Journal of Network Security, 10, 216-222.

Ahmad Almogren, Irfan Mohiuddin, Ikram Ud Din, Hisham Al Majed, and Nadra Guizani. Ftm-iomt: Fuzzy-based trust management for preventing sybil attacks in internet of medical things. IEEE Internet of Things Journal, 2020.

Akbanov, M., Vassilakis, V. G., & Logothetis, M. D. (2019a). WannaCry Ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. Journal of Telecommunications and Information Technology, 1(2019), 113-124. https://doi.org/10.26636/jtit.2019.130218

Akbanov, M., Vassilakis, V. G., & Logothetis, M. D. (2019b). Ransomware detection and mitigation using software-defined networking: The case of WannaCry. Computers & Electrical Engineering, 76, 111-121. https://doi.org/10.1016/j.compeleceng.2019.03.012

Akbanov, M., Vassilakis, V., Moscholios, I. D., & Logothetis, M. D. (2018). Static and dynamic analysis of WannaCry ransomware. ResearchGate. https://www.researchgate.net/publication/332144343_Static_and_Dynamic_Analysis_of_WannaCry_Ransomware

Ali, A.; Pasha, M.F.; Ali, J.; Fang, O.H.; Masud, M.; Jurcut, A.D.; Alzain, M.A. Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography. Sensors 2022, 22, 528.

Almalawi, A., Khan, A. I., Alsolami, F., Abushark, Y. B., & Alfakeeh, A. S. (2023). Managing security of healthcare data for a modern healthcare system. Sensors, 23(7), 3612. https://doi.org/10.3390/s23073612

Alsubaei, F. S., Abuhussein, A., Shandilya, V., & Shiva, S. G. (2019). IOMT-SAF: Internet of Medical Things Security Assessment Framework. Internet of Things, 8, 100123. https://doi.org/10.1016/j.iot.2019.100123

Anuradha, M., Jayasankar, T., Prakash, N. B., Sikkandar, M. Y., Hemalakshmi, G. R., Bharatiraja, C., & Britto, A. S. F. (2021). IoT enabled cancer prediction system to enhance the authentication and security using cloud computing. Microprocessors and Microsystems, 80, 103301. https://doi.org/10.1016/j.micpro.2020.103301

Berr, J. (2017, May 16). "WannaCry"□ ransomware attack losses could reach $4 billion. CBS News. https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/

Betafred,Msmbaldwin,Justinha,tfosmark,martyav,Microsoft Security Bulletin MS17-010 - Critical.,2017

Butson, Christopher R., et al. "Patient-specific analysis of the volume of tissue activated during deep brain stimulation." Neuroimage 34.2 (2007): 661-670.

Cabaj, K., & Mazurczyk, W. (2016). Using Software-Defined networking for ransomware mitigation: the case of CryptoWall. IEEE Network, 30(6), 14-20. https://doi.org/10.1109/mnet.2016.1600110nm

ÇELİKTAŞ, Barış. (2018) "ISTANBUL TECHNICAL UNIVERSITYâ˜… INFORMATICS INSTITUTE." .

Chaudhury, D. (2020). Brainjacking - The Shocking Cyber Security Threat in Healthcare. ITSecurityWire. https://itsecuritywire.com/featured/brainjacking-cybersecurity-threat/

Cisomag. (2022, February 28). How brainjacking became a new cybersecurity risk in health care. CISO MAG | CyberSecurity Magazine. https://cisomag.com/how-brainjacking-became-a-new-cybersecurity-risk-in-health-care/

Contreras, L. M., Truong, N. D., Eshraghian, J. K., Xu, Z., Huang, Z., Nikpour, A., & Kavehei, O. (2023). Neuromorphic Neuromodulation: Towards the next generation of on-device AI-revolution in electroceuticals. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2307.12471

D. Storm, MEDJACK, Hackers hijacking medical devices to create backdoors in hospital networks, Comput.World,(2015),p.8 https://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html (Accessed 19 February 2018).

Greenberg, A. (2019, November 5). How the Worst Cyberattack in History Hit American Hospitals. Slate Magazine. https://slate.com/technology/2019/11/sandworm-andy-greenberg-excerpt-notpetya-hospitals.html

Hamouda, B. E. H. H. (2020). Comparative study of different cryptographic algorithms. Journal of Information Security, 11(03), 138-148. https://doi.org/10.4236/jis.2020.113009

Haque, Nur Imtiazul, et al. "A novel framework for threat analysis of machine learning-based smart healthcare systems." arXiv preprint arXiv:2103.03472 (2021).

Hockey, A. (2020). Uncovering the cyber security challenges in healthcare. Network Security, 2020(4), 18-19. https://doi.org/10.1016/s1353-4858(20)30046-5

I. Thompson, "Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide,"□ The Register, 28-Jun-2017. [Online] Available: https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/

Jones, S. (2017, May 12). What is WannaCry and how can it be stopped? Financial Times. https://www.ft.com/content/af74e3f4-373d-11e7-99bd-13beb0903fa3

Jump, Michelle. "Fighting cyberthreats with technology solutions." Biomedical instrumentation & technology 53.1 (2019): 38-43.

Karule, K.P. and Nagrale, N.V. (2016) Comparative Analysis of Encryption Algorithms for Various Types of Data Files for Data Security. International Journal of Scientific Engineering and Applied Science, 2, 495-498.

Kirsch, Zach, and Ming Chow. "Quantum computing: The risk to existing encryption methods." Retrieved from URL: http://www. cs. tufts. edu/comp/116/archive/fall2015/zkir sch. pdf (2015).

Koujalagi, Ashok, Shweta Patil, and Praveen Akkimaradi. "The wannacry ransomeware, a mega cyber attack and their consequences on the modern india." International Journal of Management Information Technology and Engineering 6.4 (2018): 1-4.

L. Pycroft, S.G. Boccard, S.L.F. Owen, J.F. Stein, J.J. Fitzgerald, A.L. Green, T.Z. Aziz, Brainjacking implant security issues in invasive neuromodulation, World Neurosurg. 92 (2016)454-462, http://dx.doi.org/10.1016/j.wneu.2016.05.010

L.Evenstad, NHS trust recovers after cyber-attack, Comput. Wkly, (2016) http://www.computerweekly.com/news/450402278/NHS-trust-recovers-after-cyber-attack (Accessed 19 February 2018).

Laiphrakpam, D. S., and Khumanthem, M. S.,Medical image encryption based on improved ElGamal encryption technique. Optik 147:88-102, 2017.

Lika, Reyner Aranta, et al. "NotPetya: cyber attack prevention through awareness via gamification." 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE). IEEE, 2018.

M. Smith, MEDJACK 2: Old malware used in new medical device hijacking attacks to breach hospitals, Network World. (2016). https://www.csoonline.com/article/556739/medjack-2-old-malware-used-in-new-medical-device-hijacking-attacks-to-breach-hospitals.html

Meggitt, Sinclair. "Medjack attacks: The scariest part of the hospital." (2018).

Mohurle, S., & Patil, M. (2017). A brief study of Wannacry Threat: Ransomware Attack 2017. International Journal of Advanced Research in Computer Science, 8(5), 1938-1940. https://doi.org/10.26483/ijarcs.v8i5.4021

Monday's Ransomware Attack Fails to Dent India, Says Minister: 10 Facts. (n.d.). NDTV.com.,2017 https://www.ndtv.com/india-news/ransomware-wannacry-surfaces-in-kerala-bengal-10-facts-1693806

N.C.S. Centre, 10 Steps to Cyber Security, (2016).

National Audit Office. Investigation: WannaCry cyber-attack and the NHS. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf (2017).

OGU, R. E. "MITIGATING THE HARMFUL EFFECTS OF RANSOMWARE: THE AMALGAMATED APPROACH."

P. Farrell, The Medicare machine: patient details of any Australian for sale on darknet, Guard, (2017) https://www.theguardian.com/australia-news/2017/jul/04/the-medicare-machine-patient-details-of-any-australian-for-sale-on-darknet (Accessed 2 March 2018).

Pycroft, L., Boccard, S., Owen, S., Stein, J., FitzGerald, J. J., Green, A. L., & Aziz, T. Z. (2016). Brainjacking: Implant security issues in invasive neuromodulation. World Neurosurgery, 92, 454-[472. https://doi.org/10.1016/j.wneu.2016.05.010

Rashmi V Deshmukh and Kailas K Devadkar. Understanding ddos attack & its effect in cloud environment. Procedia Computer Science, 49:202- 210, 2015.

Rathore, H., Al-Ali, A., Mohamed, A., Du, X., & Guizani, M. (2017). DLRT: Deep Learning Approach for Reliable Diabetic Treatment. GLOBECOM 2017-2017 IEEE Global Communications Conference. https://doi.org/10.1109/glocom.2017.8255028

Rathore, H., Wenzel, L., Al-Ali, A., Mohamed, A., Du, X., & Guizani, M. (2018). Multi-Layer Perceptron model on chip for secure diabetic treatment. IEEE Access, 6, 44718-44730. https://doi.org/10.1109/access.2018.2854822

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. Healthcare, 8(2), 133. https://doi.org/10.3390/healthcare8020133

Shankar K. and Eswaran P. (2018). RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography. China Commun Vol. 14 No. 2,118-130.

Shankar, K., and Eswaran, P., Sharing a secret image with encapsulated shares in visual cryptography. Procedia Comput. Sci. 70: 462-468, 2015.

Staff, R. (2017, June 21). Honda halts Japan car plant after WannaCry virus hits computer network. U.S. https://www.reuters.com/article/us-honda-cyberattack-idUSKBN19C0EI

Storm D. MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks. https://www.computerworld.com/article/2932371/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html (2015). Accessed 15 Dec 2020.

T. Wehbe, V. Mooney, A. Javaid, and O. Inan. A novel physiological features-assisted architecture for rapidly distinguishing health problems from hardware trojan attacks and errors in medical devices. In IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pages 106-109, 2017.

Thilagam, K., Beno, A., Lakshmi, M., Wilfred, C. B., George, S. M., Karthikeyan, M., Vijayakumar, P., Ramesh, C., & Karunakaran, P. (2022). Secure IoT Healthcare Architecture with Deep Learning-Based Access Control System. Journal of Nanomaterials, 2022, 1-8. https://doi.org/10.1155/2022/2638613

Vahab Pournaghshband, Majid Sarrafzadeh, and Peter Reiher. Securing legacy mobile medical devices. In International Conference on Wireless Mobile Communication and Healthcare, pages 163-172. Springer, 2012

What is WannaCry ransomware? (2023, July 6). www.kaspersky.com. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

Wikipedia contributors. (2023). WannaCry ransomware attack. Wikipedia. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#Affected_organisations

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília

Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET