CYBERSECURITY THREATS FOR MEDICAL IMAGING DEVICES: A SYSTEMATIC REVIEWE

Shakeel Ahmed[1]*,
[0009-0001-8508-819X]
Samina Khalid[1],
[0000-0003-4771-6842]
Yasir Mehmood[1],
[0000-0003-3074-8944]
Modestus O. Okwu[2]
[0000-0002-7761-9659]

[1]Mirpur University of Science and Technology,
Mirpur, Azad Kashmir, Pakistan

[2]Federal University of Petroleum Resources Effurun,
Warri, Nigeria

Abstract:

The innovation and modernization in healthcare infrastructure have been achieved by employing IT infrastructure in public healthcare setups ranging from Hospital Information System (HIS) to all the digital gadgetries which are helping medical facilities to achieve more productivity. The use of digital medical imaging devices in advanced diagnostic systems has enhanced diagnostic precision and refined disease treatment. On the other hand, these developments also introduced a new challenge of cybersecurity issues, such as data breaches, unauthorized access, and ransomware attacks on healthcare facilities. A systematic literature review was performed across prominent databases, concentrating on recent developments in cybersecurity for medical imaging. Despite growing concerns, a comprehensive analysis of cybersecurity risks and countermeasures specific to medical imaging devices remains scarce. This review aims to bridge this gap by systematically analyzing existing threats, vulnerabilities, and mitigation strategies. The potential risks, precautionary measures, protocols, and probable mitigation strategies are highlighted in detail.

Keywords:

Medical Imaging, Digital Imaging and Communications in Medicine (DICOM), Picture Archiving and Communication System (PACS), Cyber Security, Artificial Intelligence.

INTRODUCTION

Medical imaging devices are increasingly vulnerable to cyber threats like data breaches, image manipulation, and ransomware, putting patient safety at risk. With healthcare relying more on AI-driven diagnostics, securing these systems is crucial to prevent misdiagnoses, protect patient privacy, and maintain trust in medical technology. The advent of medical imaging technologies like Magnetic Resonance Imaging (MRI), Computed Tomography (CT) scan and X-Ray help medical practitioners to diagnose problems in patients in a more timely and effective manner. Since their advent and employment in the medical field the potential security concerns have also increased. Today, medical imaging devices are under serious threats by attackers who with their criminal instincts try to hack into hospital networks.

Correspondence:
Shakeel Ahmed

e-mail:
shakeel803@gmail.com

DOI: 10.15308/Sinteza-2025-23-28

Digital medical imaging technologies, including MRI, CT, and X-ray apparatus, have transformed contemporary healthcare by facilitating accurate diagnosis and treatment strategies. Nonetheless, their escalating connectivity with hospital networks, cloud storage, and AI-driven diagnostics has rendered them great targets for assaults. Ransomware assaults represent a significant concern, as malicious software encrypts image data, making it inaccessible until a ransom is remitted. Such assaults can impede hospital operations, postpone critical medical treatments, and jeopardize patient safety. Despite the increasing prevalence of ransomware events in healthcare, the particular vulnerabilities of medical imaging devices continue to be an inadequately examined domain in cybersecurity research. This study offers an extensive analysis of ransomware attacks aimed at imaging systems, examines their attack methodologies, and evaluates novel defense techniques to maintain data integrity and ensure continuity of patient care.

Although current research addresses cybersecurity issues in healthcare, the majority concentrates on general hospital networks or electronic health records, thereby neglecting medical imaging devices. The growing use of AI and cloud storage in imaging systems creates new risks, like attacks on diagnostic models and ransomware targeting these devices. However, there is a lack of comprehensive reviews that systematically analyze these specific risks, their real-world implications, and potential mitigation strategies. This review aims to bridge this gap by providing an in-depth analysis of cybersecurity threats unique to medical imaging devices and proposing future research directions to enhance their security.

A document released by the US Department of Justice indicates that 4,000 ransomware attacks have been recorded daily since 2016[1] which is four times increase as compared to 2015. Out of all global ransomware attacks, 15% were attacking healthcare facilities in 2017. As far as the cyber security related to medical imaging devices is concerned, the primary and possibly most evident aspect of cybersecurity is physical security; technical mitigation strategies such as passwords, antivirus software, or detailed user permissions are ineffective if an intruder can easily access a server room and abscond with computers or storage devices [1].

DICOM is a standard for storing and transmitting medical images and related information. DICOM standards are developed by The American College of Radiology (ACR) and The National Electrical Manufacturers Association (NEMA) in 1985. DICOM governs the standards to store and transfer data of medical imaging in healthcare facilities.

PACS is a medical imaging technology that stores, retrieves, and transmits digital medical images and reports. PACS systems are used in healthcare organizations to replace the need for film jackets by electronically storing and transmitting images and reports.

While we talk about the cyber security threats related to digital imaging in the medical field, we are concerned about all the aspects that can pose a risk to the DICOM or PACS based infra structure of any healthcare facility. Cybersecurity threats have been increasing as hospitals become more attractive targets for cybercriminals. This is because healthcare organizations are often willing to pay higher ransoms to protect their reputation and maintain the trust of their patients and stakeholders.

Safeguarding healthcare facilities is of paramount importance so as to safeguard the personal patient data as well as the IT infrastructure of healthcare facilities. Hospitals within the United Kingdom's National Health Service, impacted by the WannaCry ransomware attacks in May 2017, were compelled to postpone treatment plans and redirect arriving ambulances due to the loss of access to hospital information systems [2]. Cyberattacks pose a significant risk to numerous hospital services, including surgeries and medication distribution, by compromising sophisticated devices such as blood-product refrigerators, imaging apparatus, automated drug dispensers, and electronic health records, in addition to essential support systems like heating, ventilation, and air conditioning (HVAC) [2]. An individual's health information is considerably more valuable on the dark web than their social security number or credit card number, perhaps selling for 10 to 20 times more than such data [2].

The healthcare sector is increasingly becoming a prime target for cyber-attacks. A survey of 223 organiztions revealed that 81% were impacted by cyber-attacks, and more than 110 million patients in the USA had their data exposed in 2015 [3]. The utilization of end-of-life software presents a heightened danger, as evidenced by assaults on healthcare providers, like the Irish Health Service Executive's "Conti" and the UK National Health Service's "WannaCry" ransomware incidents [3].

Optimal cybersecurity necessitates a collaborative approach, making it essential for the people working in healthcare field to remain cognizant of their responsibilities in individual as well as group regarding the security of healthcare facility they work for. Storage and transmission of various confidential data elements, including medical history, dates of birth and financial information is mandatory in radiological diagnosis and

other healthcare procedures. Consequently, healthcare organizations face monetary, legal, and reputational risks if information security is breached [4]. Healthcare data breaches in the US involving 500 or more patients are reported by the responsible organizations publicly and an upward trend has been witnessed since 2014. Although, the incidents of such breaches in radiology and digital imaging procedures are in low fraction, yet there has been an upward trend [4]. The medical imaging environments are implementing multiple techniques including De-identification of medical images, securing DICOM and PACS transmission, encrypting the image data completing before transferring, digital signature, watermarking etc [1].

One of the biggest challenges for any organization is the lack of IT knowledge among the medical workforce. In the study [5], the author has discussed in detail all the must to know factors of the DICOM infrastructure and has also proposed a simulation-based approach to implement, study and diagnose potential risks in a DICOM-based network setting.

This review paper is further divided in sections. In Section 2, general cyber security considerations will be discussed in detail. In section 3 the cyber security risks related to the DICOM and PACS based medical imaging infrastructure will be discussed. Section 4 is a discussion on available options to safeguard the digital imaging devices and lastly the conclusion of the paper is discussed in section 5.

2. CYBER SECURITY: GENERAL CONSIDERATIONS

Cyber security is one of the emerging fields of computer science which deals with safety of computer systems against the criminal intents. One of the common cyber security threats is DoS (Denial of Service) attack in which attackers over flood any organization's IT infrastructure with unreal requests and the system could slow down and the genuine users may face access problems. Similarly, the attacks to steal data and sell it on dark web is another common aspect of cyber security. In the analysis of various industries, DoS attacks represent the predominant form of cybersecurity incidents, accounting for over 50%. Although these attacks are disruptive, they generally do not lead to unauthorized access to data [4].

In addition to DoS and malware, various other mechanisms may compromise data security. Privilege escalation is the enhancement of access rights of a legitimate user, such as increasing the access to an administrator-level account is very dangerous as it enables a user to install and execute malicious software. Eavesdropping attacks involve the unauthorized observation or alteration of information shared between two devices by masquerading as an intermediary, while cryptographic attacks aim to uncover hidden data. Significant volumes of data are exchanged and saved across multiple electronic systems daily in X-Ray and radiology departments of healthcare facilities. Privacy of patients and confidentiality are exposed to high risks due to such attacks, potentially compromising sensitive institutional data or proprietary information [4].

3. CYBER SECURITY CHALLENGES TO MEDICAL IMAGING DEVICES

3.1. IMPORT OF PATIENT DATA

A malware infected storage media used for transferring medical images can import all patient data when used with the healthcare's IT infrastructure to conduct the study. In many scenarios, the patient can bring along a storage media in which the studies of their scans (conducted by another entity) are present that need to be evaluated. In this case, the data available on the hospital network could be breached. To overcome this, the viewers used by the 3rd party must not be allowed to autorun rather own viewers be used to view the studies. Most systems that create DICOM CDs also write an executable viewer that could be a potential risk as well.

3.2. HACKING OF THE HOSPITAL NETWORK

The infiltration of hospital networks presents a substantial and escalating risk to patient safety, data confidentiality, and the entire operation of healthcare systems. As hospitals increasingly depend on interconnected technologies, including medical imaging apparatus, Electronic Health Records (EHR), and other essential infrastructure, cyberattacks such as ransomware, data breaches, and system intrusions are evolving in sophistication and severity. These breaches jeopardize patient care and disrupt hospital operations, resulting in financial losses and regulatory penalties. Healthcare institutions must have comprehensive cybersecurity frameworks that encompass robust network segmentation, regular system updates, stringent access control measures, and continuous monitoring to safeguard against the constantly expanding cyber threat scenario. Securing hospital networks is imperative; it is essential for preserving trust in healthcare systems and safeguarding

the security and privacy of sensitive patient information. This is the worst situation in which cyber criminals get access to the hospital's LAN using an unprotected port or compromising a wireless device. Once the hacker has access to the network, he could passively monitor all the traffic over the network. The data transferred over DICOM and HL7 version 2 is in plain text format and the hacker can use some packet analyzer to sniff all the data and gather all the information about images, patient data and the network addressing of the DICOM servers. When the attacker knows address of all the servers, he could easily gain unauthorized access to servers and can manipulate highly sensitive and confidential data.

3.3. MANIPULATION OF MEDICAL IMAGES WITH A MALICIOUS INTENT

With the advent and progression of Artificial Intelligence (AI), the image manipulation techniques have evolved at a skyrocketing speed. Deep Fake can be used to corrupt the medical images of patients and expert radiologists may remain unable to sense the forged and actual images. This forgery can be life threating as the diagnosis may go astray. Steganography is used to protect original files so that the data can't be manipulated by the hackers. Steganography pertains to the concealing of confidential information, encompassing its storage and transmission. A variety of digital artifacts have been examined concerning both steganography application and its detection, including digital text, photos, videos, audio files, filesystems, cyber-physical systems, and networks [6].

Mirsky et al. state that "to verify the threat of this attack, we trained CT-GAN to inject/remove lung cancer and hired three radiologists to diagnose a mix of 70 tampered and 30 authentic CT scans. The experiment was performed in two trials: blind and open. In the blind trial, the radiologists were asked to diagnose 80 complete CT scans of lungs, but they were not told the purpose of the experiment or that some of the scans were manipulated. In the open trial, the radiologists were told about the attack, and were asked to identify fake, real, and removed nodules in 20 CT scans. In addition, the radiologists were asked to rate the confidence of their decisions." The results were quite impressive: in the blind trial, "the radiologists diagnosed 99% of the injected patients with malignant cancer, and 94% of cancer removed patients as being healthy. After informing the radiologists of the attack, they still misdiagnosed 60% of those with injections, and 87% of those with removals [7]".

4. CYBER SECURITY PROTOCOLS TO MITIGATE THE RISKS

4.1. SEGMENTATION OF THE NETWORK

It is a process of distributing the bigger networks into smaller easy to manage and troubleshoot networks. The network segmentations help in safeguarding the complete network of healthcare facilities when one segment is compromised. We just need to shut down that specific segment and keeping rest of the healthcare IT infrastructure.

Local area network (LAN) could be laid down by a college or university to restrict access to on-campus computers and to isolate it from public internet. On similar lines, devices installed at homes are maintained on a local area network and separation is achieved from the internet. Network segmentation and segregation enable enterprises to enhance security standards and/or restrict access to devices with elevated security requirements, thereby isolating essential segments of network traffic from non-essential traffic Enterprises use Network segmentation and segregation to improve security protocols and to restrict unauthorized access to the devices which need more confidentiality. Using this technique organizations segregate their essential and non-essential network traffic [4].

4.2. REGULAR BACKUPS

ENISA (European Union Agency for Network and Information Security) recommends the performance of regular backups. "This very important action can solve many attacks that could cause great impacts to smart hospitals such as ransomware or physical attacks. Running regular full or incremental backups can be done combined with setting a hot or warm site, making the hospital systems resilient even in the case of natural disaster [1]." Although regular backups do not act as an active measure to safeguard the network, with the help of regular backups, we could ensure the availability of the most recent data in case of the data breach or theft. This will ensure that healthcare facility is having most recent data with them somewhere at a cold backup storage facility from where the loss could be mitigated in case of any unforeseen scenarios.

4.3. USE OF ENCRYPTION TECHNIQUES

Various encryption techniques are being used to safeguard the personal identity information of patients while transferring data using DICOM and PACS infrastructures. Extensive efforts have been undertaken to protect the data during transmission to ensure its integrity is preserved. One of the developed techniques is the application of steganographic methods to the DICOM Message Service and Upper Layer Service to establish hidden channels [5]. A simple XOR based encryption technique has been introduced in which reduced the encryption decryption times for multi-frame DICOM-based images [8].

One of the major challenges of encryption is that huge amount of computing is required to encrypt and decrypt the heavy DICOM images. In a study [9], a lightweight two permutation-based algorithm to encrypt medical images is proposed. The security and execution time of the suggested method are examined, assessed, and then contrasted with those of traditional encrypted methods. The performance of the suggested approach has been evaluated using a large number of test photos. Numerous tests demonstrate that the suggested approach outperforms traditional methods in terms of efficiency for picture cryptosystems.

4.4. AUTHENTICATION AND ACCESS MANAGEMENT

Access permissions and user authentication procedures serve as a crucial barrier to unauthorized system access. A prevalent cybersecurity measure is to refrain from utilizing accounts with administrative capabilities unless explicitly necessary for actions such as software installation or updates. This access significantly increases cybersecurity risks compared to accounts with restricted access, and the concept of least privilege must be adhered to when providing users access to electronic resources. Protocols for minimum password strength and the frequency of password alterations can be established to protect against unwanted access to the DICOM and PACS systems. Latest security trends such as multi-factor authentication, role-based access control, and Zero Trust security models must be adopted to safeguard the DICOM and PACS systems installed at healthcare facilities. If we overlook these aspects and keep the system open to all without proper access rights, we are inviting the wrong doers to attack and gain the access to the healthcare network.

4.5. DISABLING UNUSED PHYSICAL PORTS

If the PACS server is having unused open ports, there is a high probability that a criminal can get advantage of it to sneak into the sensitive information of patients using techniques. An impeccable defense against a hacker infiltrating the hospital network will be of minimal utility if the PACS server is entirely accessible and responds to inquiries from across the Internet. As most of the end users of Digital Medical Imaging devices are people who do not have knowledge of the cyber security practices, we can't blame those people. The IT teams employed at healthcare facilities must strive hard to ensure that deployed systems are not prone to such attacks where the unused ports could be manipulated to gain access to hospital networks. This is, unfortunately, not a theoretical issue. A 2019 investigation revealed that numerous PACS systems worldwide are vulnerable to Internet access due to an absence of fundamental IT security protocols [1].

5. CONCLUSION

This systematic review sought to examine the emerging cybersecurity threats to medical imaging devices and evaluate current vulnerabilities, possible dangers, and mitigation options within healthcare systems. As the integration of digital technologies such as DICOM and PACS becomes more widespread, these systems have become prime targets for cyberattacks—including ransomware, unauthorized access, and image manipulation—which can severely impact patient safety and healthcare operations. Our findings indicated that numerous healthcare facilities continue to function with outdated systems, unsecured network ports, and insufficient user training, rendering them progressively vulnerable to both internal and external attacks. The review emphasizes various effective defense systems, including network segmentation, routine system backups, encryption methods, and stringent authentication and access control procedures. Moreover, forthcoming initiatives should concentrate on closing the knowledge gap among healthcare personnel, using AI-based security solutions, and enforcing uniform cybersecurity protocols. Enhancing these domains is crucial for safeguarding sensitive medical information, ensuring system accessibility, and maintaining trust in the digital evolution of healthcare.

REFERENCES

[1] M. Eichelberg, K. Kleber, and M. Kämmerer, "Cybersecurity in PACS and Medical Imaging: an Overview," *J. Digit. Imaging*, vol. 33, no. 6, pp. 1527–1542, Dec. 2020, doi: 10.1007/s10278-020-00393-3.

[2] S. T. Argaw et al., "Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks," *BMC Med. Inform. Decis. Mak.*, vol. 20, no. 1, p. 146, Dec. 2020, doi: 10.1186/s12911-020-01161-7.

[3] B. S. Kelly, C. Quinn, N. Belton, A. Lawlor, R. P. Killeen, and J. Burrell, "Cybersecurity considerations for radiology departments involved with artificial intelligence," *Eur. Radiol.*, vol. 33, no. 12, pp. 8833–8841, Jul. 2023, doi: 10.1007/s00330-023-09860-1.

[4] X. V. Nguyen, J. M. Petscavage-Thomas, C. M. Straus, and I. Ikuta, "Cybersecurity in radiology: Cautionary Tales, Proactive Prevention, and What to do When You Get Hacked," *Curr. Probl. Diagn. Radiol.*, p. S0363018824001221, Jul. 2024, doi: 10.1067/j.cpradiol.2024.07.010.

[5] S. Karagiannis, E. Magkos, C. Ntantogian, R. Cabecinha, and T. Fotis, "Cybersecurity and Medical Imaging: A Simulation-Based Approach to DICOM Communication," *Appl. Sci.*, vol. 13, no. 18, p. 10072, Sep. 2023, doi: 10.3390/app131810072.

[6] A. Mileva, A. Velinov, V. Dimitrova, L. Caviglione, and S. Wendzel, "Information Hiding in the DICOM Message Service and Upper Layer Service with Entropy-Based Detection," *Entropy*, vol. 24, no. 2, p. 176, Jan. 2022, doi: 10.3390/e24020176.

[7] M. Eichelberg, K. Kleber, and M. Kämmerer, "Cybersecurity Challenges for PACS and Medical Imaging," *Acad. Radiol.*, vol. 27, no. 8, pp. 1126–1139, Aug. 2020, doi: 10.1016/j.acra.2020.03.026.

[8] Q. N. Natsheh, B. Li, and A. G. Gale, "Security of Multi-frame DICOM Images Using XOR Encryption Approach," *Procedia Comput. Sci.*, vol. 90, pp. 175–181, 2016, doi: 10.1016/j.procs.2016.07.018.

[9] M. K. Hasan et al., "Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications," *IEEE Access*, vol. 9, pp. 47731–47742, 2021, doi: 10.1109/ACCESS.2021.3061710.