MISJ-International Journal of Medical Research and Allied Sciences
Online ISSN: **2584-1432**
Available Online at https://ijmraas.misj.net **Volume 03|Issue 01** (January to April) |2025 Page: 07-13

Review Paper

Data transfer protocols and security in wireless dicom transmission for cath labs

Authors:
Kothwala Dr. Deveshkumar Mahendralal, Shaikh Amirhamzah Mahmadiqbal, Khalifa Haroonmohammad Rasidmohammad, Bhavsar Girakumari Rajubhai
Meril Medical Innovations Private Limited, Bilakhia House, Survey no.879, Muktanand marg, Chala, Vapi, Dist-Valsad, Gujarat, 396191, India.
Corresponding Author*:*
Khalifa Haroonmohammad Rasidmohammad

Article Received: 10-December-2024, Revised: 01-January-2025, Accepted: 20-January-2025

ABSTRACT:
Continuous communication and medical image acquisition are essential in catheterization labs (Cath Labs), and wireless technology in Digital Image and Communications in Medicine (DICOM), is facilitating this transformation. This move has made healthcare operations more efficient by providing rapid access to patients' information, resulting in improved decisions and results. However, this new transformation has its own set of issues, including concerns regarding the security and privacy of critical patient data during transmission. To ensure the integrity of this information while maintaining its confidentiality, we rely on modern encryption techniques, secure transfer protocols, and follow applicable rules. Several protocols, including DICOM over HTTP/HTTPS, provide secure and efficient data delivery. In addition, regular audits and proper user authentication can significantly reduce vulnerabilities and threat of data loss. The present review article discusses the significance of wireless DICOM transmission for the enhanced Cath Lab workflows, along with the security threats and the countermeasures needed to secure medical data.

Keywords: Wireless DICOM, Cath Labs, WorkFlow, Data Security, Encryption, Digital Signatures, Access Control, Network Security, HIPAA, GDPR, Quantum Cryptography, AI in Security, Zero-Trust Security, Blockchain in Healthcare

INTRODUCTION:

The use of wireless technology in catheterization laboratories is not new, its use has transformed the method in which we communicate and access medical imaging data in recent years. This shift in the way patient information is shared has optimized the flow of data amongst healthcare providers, however it has also introduced destructive questions of the safety and fidelity of sensitive patient data in transit (Cusma & Bashore, 1996). With the increased dependency of healthcare institutions on wireless DICOM communication, it is vital that suitable security measures are taken to secure patient data against any compromises, as well as adhering to law. Data at rest and in transit both need to be protected and maintain the confidentiality and integrity of the patient information throughout the imaging chain process, so different encryption techniques and secure communication protocols have to be applied. By implementing these security measures, one will not only be able to mitigate the risks of data violations but also foster trust in the patients, assuring them their sensitive information is being handled with utmost care and protection. It is also essential to build a culture of security awareness within the healthcare leaders, as training people to identify threats and adheres to best practices, can go a long way in reducing human error leading to data vulnerabilities (Lim, 2008).

Wireless transfer of DICOM could eventually lower procedural time and improve imaging workflows. By reducing the amount of data that needs to be transmitted, healthcare providers can provide faster access to essential patient information, which ultimately leads to shorter diagnosis and treatment cycles — while still upholding rigorous security measures (Maani et al., 2010). Data is transferred in real-time throughout procedures, enabling physicians to make informed decisions in real time, quickly adjusting interventions and changes based indeed on the most current patient data available. One of the key aspects of this is the ability to make the right decisions about the patient health condition. Not only are such developments great for speeding workflow, but making data available for treatment far faster translates not only into better easy-of-care, but ultimately better treatment and outcomes over time. Effective communication among team members also helps in ensuring that the same message is communicated to help clinicians work collaboratively in the best interest of patients (Kush, 2012).

Data Transfer Protocols in Wireless DICOM Transmission:

The data transfer protocols in wireless DICOM transmission facilitate the secure and efficient exchange of medical images and related information among healthcare professionals. These protocols ensure that diagnostic data can be accessed in real-time, allowing for fast and informed decision-making by clinicians while still adhering to patient privacy and regulatory requirements.

Wireless DICOM transmission for Cath Labs typically uses one of several data transfer protocols, including "DICOM over Hypertext Transfer Protocol (HTTP/HTTPS) (DICOMweb), DICOM over Transport Layer Security (TLS), and DICOM over Transmission Control Protocol/Internet Protocol (TCP/IP)" with each possessing unique positives around speed, security, interoperability and seamless integration into existing healthcare systems (Zhang, 2008).

1. DICOM over HTTP/HTTPS (DICOMweb): provides a simpler way to transfer medical images, using the widely used HTTP protocol to allow devices to communicate and increase compatibility with web-based applications and services in healthcare environment (Genereaux et al., 2018).

2. DICOM over TLS: This is a secure method of transmitting medical images over the web, which would encrypt the data during transfer, so no one would be able to decrypt the information without permission while in transit. It will ensure that only internal hospital machines are allowed to connect and acquired images are sent to the correct machine (Zhang, 2008).

3. DICOM over TCP/IP: is a standard protocol used in the medical imaging field to facilitate the transfer, storage, and sharing of images and related information across different devices and systems over a network. This protocol ensures interoperability between various medical imaging equipment, allowing healthcare professionals to access and exchange critical diagnostic information seamlessly (Zhang, 2008).

Protocol	Description	Advantages	Disadvantages
DICOM over HTTP	Utilizes the ubiquitous HTTP protocol. Ideal for web-based access and sharing of medical images.	Relatively simple to implement and manage.	May be less secure than TCP/IP due to the inherent nature of HTTP.
DICOM over TLS	Secure implementation of the DICOM protocol, where the standard DICOM traffic is encrypted and transmitted over a TLS layer.	Highly secure due to encryption.	May add complexity to implementation and management.
DICOM over TCP/IP	Leverages the reliable and efficient TCP/IP protocol stack. Well-suited for both wired and wireless networks (Wi-Fi, cellular).	Flexible and customizable.	More complex to implement and configure.

Together, these protocols help streamline healthcare data management and facilitate interoperability between different systems and devices.

Figure 1: Presents the overall communication methodology, which includes both network (online) and media storage exchange (off-line) communication. Applications can use any of the following transport mechanisms:

The DICOM Message Service and Upper Layer Service operate independently of particular physical networking communication support and protocols such as TCP/IP.

The Basic DICOM File Service allows access to Storage Media irrespective of specific media storage types and file structures. (https://dicom.nema.org/medical/dicom/current/output/html/part01.html)

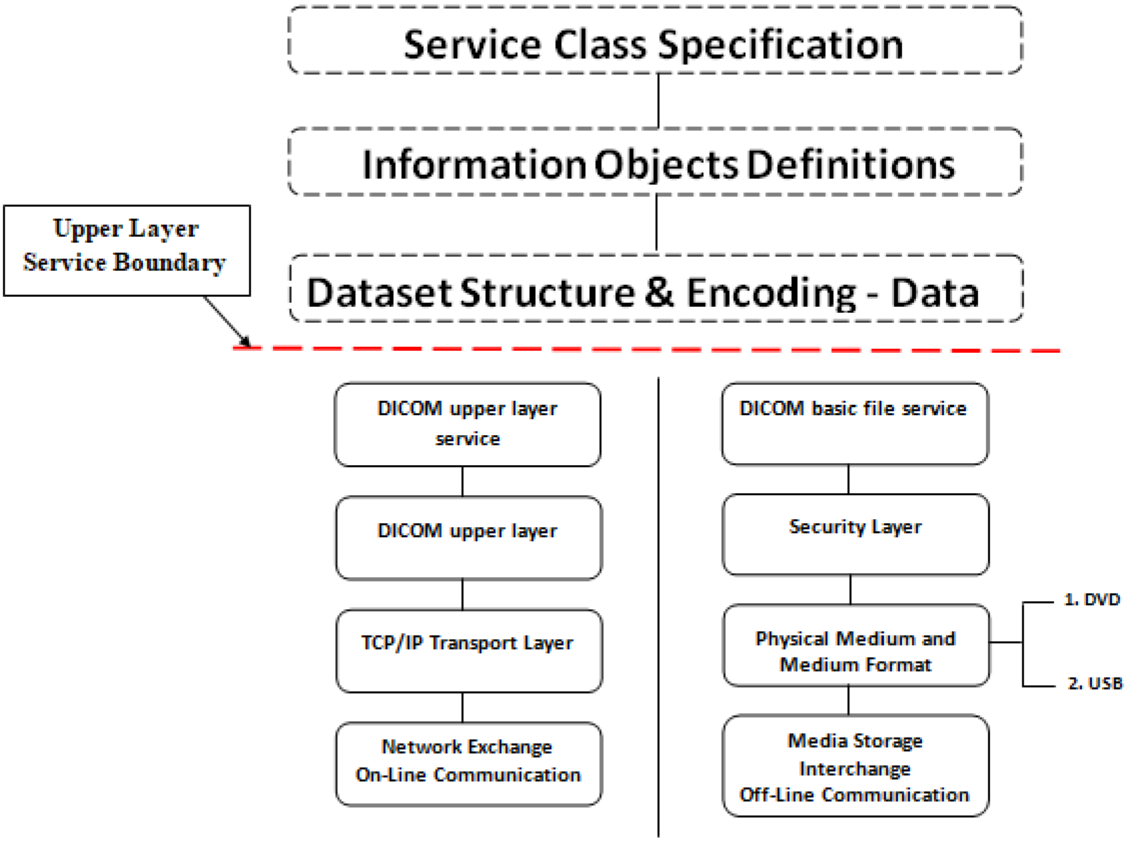
Service Class Specification
Information Objects Definitions
Upper Layer Service Boundary
Dataset Structure & Encoding - Data
DICOM upper layer service
DICOM upper layer
TCP/IP Transport Layer
Network Exchange On-Line Communication
DICOM basic file service
Security Layer
Physical Medium and Medium Format
1. DVD
2. USB
Media Storage Interchange Off-Line Communication

Figure 1: General communication model of the Standard, which spans both network (on-line) and media storage interchange (off-line) communication

As wireless DICOM transmission becomes more ubiquitous, it is essential to have full data integrity implemented to protect against attacks of this nature, such as man-in-the-middle attacks. DICOM files can be modified without detection, so they are at serious risk, especially a patient safety and treatment accuracy. Healthcare-integrated institutions can build encryption protocols along with watermarking and digital signing techniques on top of platform security services to guarantee the original quality of images being transferred. This mechanism can ensure data integrity and credibility among medical professionals, thus building trust during email communication with all the embedded secure identifiers along DICOM files and so on. Implemented together, these measures will both bolster security, and meet the increasingly stringent regulatory standards in place to safeguard sensitive health information in an ever-more interconnected digital world (Kobayashi et al., 2009).

Key Features of DICOM Communication Protocol:

DICOM is necessary for communication and transfer of medical images and information between imaging machines and healthcare devices. DICOM is known for standardizing the format and structure of medical images to make them compatible with different manufacturer's equipment and software. Finally, it's handling of different data types (one of the bases of any Medical Imaging workflow) ranges from images and reports to patients, denoting its versatility there in the management of any Medical Imagining workflow.
DICOM is designed to facilitate the efficient exchange of medical images across various devices and systems while also adhering to strict security protocols to safeguard patient information during transfer, which is crucial for complying with healthcare regulations and preserving patient privacy Lim & Zein, 2006). Security Issues in Wireless Transmission of DICOM:

There are various security challenges in Wireless DICOM transmission in Cath Labs:

Data Confidentiality: is used to manage the availability of the data, and to keep the data secure by protecting it from unauthorized access. Additionally, wireless transmissions are vulnerable to detection and monitoring. With the implantation of strong encryption standards and access control, these risks can be avoided, protecting sensitive health information during transmission (Anciaux et al., 2006).

Data Integrity:

Maintaining the integrity of medical images during transmission is vital for accurate diagnosis and treatment. Changes or corruption of the data during the transfer may result in a misdiagnosis, possibly compromising the safety of the patient. Furthermore, verification checks and digital signatures enable you to verify the integrity of transferred data, providing a level of assurance that the photos received are actually the images sent (Huang & Fang, 2011).

Authentication and Authorization: Ensuring users are who they say they are and providing them with the proper rights is a key to stopping unwanted access. Utilizing strong authentication practices like multi-factor authentication and role-based access control vastly minimizes potential breaches and keeps sensitive medical data secure (Kaul et al., 2020).

Security Challenge	Mitigation Strategies
Data Confidentiality	Strong encryption standards (e.g., AES) Secure access control mechanisms
Data Integrity	Digital signatures Hashing algorithms Data checksums
Authentication and Authorization	Strong authentication methods (e.g., multi-factor authentication), Role-based access control

<u>Strategies for Enhancing Security in Wireless DICOM Transmission</u>:

For Wireless DICOM Transmission, some possible strategies for enhanced security are the high-level encryption protocols that protect sensitive data over the low-security transmission process, the timely security audits, and the high updates of resources to keep the transmission within the safe parameters of the safe protocols, and also the detection of changes within connections that can monitor the nodes of the DICOM Transmission. It is the guarantee that this data remains secure where it can be accessed, to provide better service to patients, and to contribute to the integrity of medical information by assuring the upkeep of DICOM transmissions (Lavanya & Natarajan, 2011).

To address these challenges, various security measures can be implemented:

Encryption: Applying strong and high-level secure encryption algorithms such as the Advanced Encryption Standard (AES) is a technique in which the medical images and corresponding metadata are encrypted; thus, providing a significantly burst in the protection of data confidentiality (Neelima & Brinda, 2018).

Digital Signatures: Digital signatures can be used primarily to provide proof of the origin of the information transmitted over digital channels, as well as for the content integrity of the information that it has not undergone a change during its travel (Ramya & Suganya, 2013).

Access Control: Applying strict and well-planned access control measures ensures that only authorized individuals can view or modify sensitive medical data, thereby significantly reducing the risk of unauthorized access and minimizing the risk of critical breaches (Alshehri et al., 2016).

Network Security: According to experts in the field, you can use Wi-Fi Protected Access 3 (WPA3), the new long-awaited protocol that has better security than the previous versions. It is also recommended to have an anti-firewall to protect your not-to-fall for wrong sites, so basically it helps as another step in the prototype that cuts the security of any site that offers unauthorized access to your network and trying to infiltrate it (Zhang, 2021).

Regular Security Audits and Vulnerability Assessments: Regularly performing systematic and thorough security audits and assessments can allow us to identify, analyze, and address any existing or potential security vulnerabilities in an organization, improving our security posture (Umar & Ajmad, 2003).

User Awareness and Training: There is a remarkable opportunity to lower the risk and incidence of human error by training medical professionals on best practices in security, ultimately increasing the safety of sensitive information in a healthcare setting (Ghazvini & Shukur, 2016).

Compliance with Security Standards: With relevant security standards (like the Health Insurance Portability and Accountability Act, also known as HIPAA; and General Data Protection Regulation or, GDPR) observed by organizations, organizations can ensure and achieve the regulatory standards needed by authorities (Pi, 2000).

Security Strategy	Description
Encryption	Protecting data confidentiality using strong encryption algorithms like AES.
Digital Signatures	Verifying the authenticity and integrity of transmitted data.
Access Control	Implementing robust access control mechanisms to restrict access to authorized personnel.
Network Security	Securing wireless networks using encryption protocols and

	firewalls.
Regular Security Audits and Vulnerability Assessments	Identifying and addressing security gaps.
User Awareness and Training	Educating healthcare professionals about security best practices.
Compliance with Security Standards	Adhering to relevant security standards like HIPAA and GDPR.

DISCUSSION:

Wireless DICOM transmission is vital for improving the efficiency and efficacy of medical imaging workflows in catheterization labs. Secure and real-time data transfer makes it possible for a healthcare provider to take informed decisions with suitable measures on time, which helps improve the quality of care rendered to patients and ultimately the outcome. But, relying more on wireless communication of information about patients, we need to bring some stronger security measures to secure patient data from being violated and manipulated. Mitigation of Data Breaches Countermeasures that can be adopted include the use of strong encryption, digital signatures, access control, regular vulnerability assessments and many more security strategies. Implementing strong encryption techniques, access control, network security protocols, and security awareness initiatives not only protect patient records but also helps organizations comply with sensitive data rules. Implementing these security standards enables healthcare organizations to balance imaging operations while protecting and encrypting patient data throughout the process, establishing dynamic trust in the ever-changing digital healthcare ecosystem.

Future Directions:

Through the need and integration of the latest technologies, especially artificial intelligence and machine learning related advancement, the healthcare security domain will positively evolve and become an exponent to detect threats in real time and take immediate actions. Allowing health care organizations to process and analyze large data volumes rapidly, this advanced mix of technologies enables the detection of complex patterns and anomalies that could be early indicators of potential security breaches, giving organizations the opportunity to intervene before issues emerge into larger, more costly problems.

Future research and development in this area should focus on:

Cryptography Methods: Investigating quantum-based techniques and post-quantum approaches for improving the security of wireless DICOM communication.

Few examples of AI-powered security solutions may include:

Zero-Trust Security Architectures: The approach of avoiding the traditional security perimeter, where once a user/service is within the perimeter it is trusted, to a zero-trust security model that minimizes the attack-surfaces.

Blockchain approach: analyzing the versatility of blockchain to ensure secure and tamper-proof records of medical image transmission.

Having a layered approach to security, healthcare is able to maintain confidentiality, integrity and availability of the medical images transferred in Cath Labs wirelessly thus providing improved patient care while also protecting sensitive health information.

Abbreviations:

1. DICOM - Digital Imaging and Communications in Medicine
2. Cath Lab - Catheterization Laboratory
3. HTTP - Hypertext Transfer Protocol
4. TLS - Transport Layer Security
5. TCP/IP - Transmission Control Protocol/Internet Protocol
6. Wi-Fi - Wireless Fidelity
7. AES - Advanced Encryption Standard
8. WPA3 - Wi-Fi Protected Access 3
9. DVD - Digital Versatile Disc
10. USB - Universal Serial Bus
11. HIPAA - Health Insurance Portability and Accountability Act
12. GDPR - General Data Protection Regulation
13. AI – Artificial Intelligence

Reference:

1. Cusma, J.T., Bashore, T.M. (1996). The digital catheterization Laboratory - is it Practical Today? In: Reiber, J.H.C., van der Wall, E.E. (eds) Cardiovascular Imaging. Developments in Cardiovascular Medicine, vol 186. Springer, Dordrecht. https://doi.org/10.1007/978-94-009-0291-6_12

2. Dr. Eugene Y. S. Lim. (2008) Data Security and Protection for Medical Images. https://doi.org/10.1016/B978-012373583-6.50015-3

3. Rouzbeh Maani, Sergio Camorlinga, Neil Arnason, Rasit Eskicioglu (2010) A practical fast

method for medical imaging transmission based on the DICOM protocol https://doi.org/10.1117/12.843896

4. Kush, R.D. (2012). Data Sharing: Electronic Health Records and Research Interoperability. In: Richesson, R., Andrews, J. (eds) Clinical Research Informatics. Health Informatics. Springer, London. https://doi.org/10.1007/978-1-84882-448-5_17

5. Zhang, J. (2008). DICOM Image Secure Communication with Internet Protocols. In: Kumar, S., Krupinski, E.A. (eds) Teleradiology. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-78871-3_4

6. Genereaux, B.W., Dennison, D.K., Ho, K. *et al.* DICOMweb™: Background and Application of the Web Standard for Medical Imaging. *J Digit Imaging* **31**, 321–326 (2018). https://doi.org/10.1007/s10278-018-0073-z

7. Zhang, J. (2008). DICOM Image Secure Communication with Internet Protocols. In: Kumar, S., Krupinski, E.A. (eds) Teleradiology. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-78871-3_4

8. Luiz Octavio Massato Kobayashi, Sergio Shiguemi Furuie, and Paulo Sergio Licciardi Messeder Barreto (2009). Providing Integrity and Authenticity in DICOM Images: A Novel Approach. 10.1109/TITB.2009.2014751

9. Lim, J., Zein, R. (2006). The Digital Imaging and Communications in Medicine (DICOM): Description, Structure and Applications. In: Kamrani, A., Nasr, E.A. (eds) Rapid Prototyping. Manufacturing Systems Engineering Series, vol 6. Springer, Boston, MA. https://doi.org/10.1007/0-387-23291-5_3

10. Anciaux, N., Bouganim, L. & Pucheral, P. Data confidentiality: to which extent cryptography and secured hardware can help. *Ann. Télécommun.* **61**, 267–283 (2006). https://doi.org/10.1007/BF03219909

11. Hsiang-Cheh Huang; Wai-Chi Fang (2011). Integrity preservation and privacy protection for medical images with histogram-based reversible data hiding. 10.1109/LISSA.2011.5754168

12. Sonam Devgan Kaul; V. Kumar Murty; Dimitrios Hatzinakos (2020). Secure and Privacy preserving Biometric based User Authentication with Data Access Control System in the Healthcare Environment. 10.1109/CW49994.2020.00047

13. LAVANYA, A., NATARAJAN, V. Enhancing security of DICOM images during storage and transmission in distributed environment. *Sadhana* **36**, 515–523 (2011). https://doi.org/10.1007/s12046-011-0030-8

14. LAVANYA, A., NATARAJAN, V. Enhancing security of DICOM images during storage and transmission in distributed environment. *Sadhana* **36**, 515–523 (2011). https://doi.org/10.1007/s12046-011-0030-8

15. Tulu, Bengisu; Li, Haiqing; Chatterjee, Samir; Hilton, Brian; Beranek-Lafky, Deborah; and Horan, Thomas, "Design and Implementation of a Digital Signature Solution for a Healthcare Enterprise" (2004). AMCIS 2004 Proceedings. 43. http://aisel.aisnet.org/amcis2004/43

16. S. Alshehri, S. Mishra and R. K. Raj, "Using Access Control to Mitigate Insider Threats to Healthcare Systems," *2016 IEEE International Conference on Healthcare Informatics (ICHI)*, Chicago, IL, USA, 2016, pp. 55-60, doi: 10.1109/ICHI.2016.11.

17. Zhang P. Image Data Security Mechanism Based on the Internet of Things Cardiac Catheterization Laboratory Information Management System Research and Design. J Healthc Eng. 2021 Apr 2;2021:5592185. doi: 10.1155/2021/5592185. Retraction in: J Healthc Eng. 2023 May 24;2023:9803815. doi: 10.1155/2023/9803815. PMID: 33884159; PMCID: PMC8041532.

18. Umar, Amjad. *Information Security and Auditing in the Digital Age: A Practical Managerial Perspective*. nge solutions, inc, 2003.

19. Arash Ghazvini and Zarina Shukur, "Awareness Training Transfer and Information Security Content Development for Healthcare Industry" International Journal of Advanced Computer Science and Applications(ijacsa), 7(5), 2016. http://dx.doi.org/10.14569/IJACSA.2016.070549

20. Carter, P. I. "Applying your corporate compliance skills to the HIPAA security standard." *Journal of Healthcare Information Management: JHIM* 14.4 (2000): 13-27.

21. https://dicom.nema.org/medical/dicom/current/output/html/part01.html