International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 7, Issue 10, pp 89-96, October-2023
https://doi.org/10.47001/IRJIET/2023.710012

Ensure Security and Privacy of Medical Imaging through Secure DICOM

[1]A.N. Somasundara, [2]S.T. Jayathunge, [3]D.M.C.P. Jayasooriya, [4]E.M.H.O. Ekanayaka, [5]Kanishka Yapa, [6]Uditha Dharmakeerthi

[1,2,3,4,5,6]Department of Computer Systems Engineering, Sri Lanka Institute of Information Technology, Malabe, Sri Lanka
Authors E-mail: [1]it20195298@my.sliit.lk, [2]it20172114@my.sliit.lk, [3]it20210106@my.sliit.lk, [4]it20210342@my.sliit.lk, [5]kanishka.y@sliit.lk, [6]uditha.d@sliit.lk

***Abstract* - The study outlines some of the limitations in four selected security components in the medical imaging standard, Digital Imaging and Communications in Medicine (DICOM), and proposes a set of actions to be taken to resolve the specified issues. The critical requirement of DICOM servers for smooth hospital functionality is discussed while stressing areas such as telemedicine. Furthermore, reviews of past research have been done shedding the spotlight on existing vulnerabilities in the DICOM standard; the root cause of the vulnerabilities while demonstrating proofs of concept to better understand how to resolve the security issues. The method incorporated in presenting the fixes to the issues is discussed in technical terms, for each security component of DICOM.**

Keywords: DICOM, PACS, encryption, authentication, access control, error detection, integrity, security.

I. INTRODUCTION

The increasing presence of digital medical imaging in the healthcare industry has significantly improved patient care and its outcomes. With integrated electronic patient records, healthcare providers can easily access and analyze patient data, leading to more accurate diagnoses, improved treatment plans, and better patient outcomes. Also, remote reading of medical imaging data is one of the most popular health services nowadays, as it allows healthcare providers to access patient images from anywhere, which can be extremely useful for telemedicine and remote patient care. In addition to improving access to medical images, remote reading of medical imaging data has several other benefits such as reducing the time and costs associated with transferring physical film, reducing the risk of loss or damage to images, and improving the accuracy of image interpretation by allowing multiple healthcare providers to collaborate and consult on patient cases. However, remote reading of medical imaging data also poses some challenges such as ensuring the security and privacy of patient information during transmission and storage. This requires implementing strong encryption and access controls to prevent unauthorized access or disclosure of patient data [1].

The DICOM standard is important for enabling the safe transfer and archiving of medical images in a standard format for various healthcare providers. The DICOM standard defines a common language and a set of rules for exchanging and managing medical image data, making it easier for healthcare providers to share images and collaborate on patient care. It also includes metadata that provides important information about the images, such as patient demographics, imaging modality, acquisition parameters, and image processing history. The DICOM standard plays a critical role in improving healthcare delivery's security, efficiency, and effectiveness by enabling seamless sharing and access to medical images and related patient information. However, the greatest challenge lies in securely sharing sensitive patient information, as intrusion could allow attackers to access the patient's private information. To ensure the security and integrity of medical images and data, DICOM incorporates several security mechanisms, including error detection, encryption, access control, and authentication [2], [3].

However, there are several security issues to consider when implementing these mechanisms. Error detection mechanisms are essential in ensuring the accuracy and completeness of medical images and data, but poor implementation or configuration of these mechanisms can lead to undetected errors or data corruption, leading to medical errors or patient harm. Encryption algorithms are only effective if they are configured correctly, and access control mechanisms can also be vulnerable to security issues if not configured correctly. Misconfigured access controls can result in data being accessible to unauthorized users, leading to privacy violations and data breaches. Access control mechanisms can also be vulnerable to insider threats, where authorized users abuse their privileges to access data they are not authorized to see. Lastly, authentication mechanisms, such as password-based authentication, can be vulnerable to brute force attacks. To address these gaps, the current study proposes solutions to enhance security mechanisms, including

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 10, pp 89-96, October-2023

https://doi.org/10.47001/IRJIET/2023.710012

error detection, encryption, access control, and authentication [4].

II. LITERATURE REVIEW

In 2019, it was reported that a cybersecurity researcher was able to find a vulnerability in a DICOM file. A Cylera security researcher named Markel Picado Ortiz has been able to attach malware within a DICOM file that has run through systems undetected [5]. He had been successful in attaching the malware to the DICOM file without making any alterations to the DICOM image thus making the malware undetectable within the DICOM file. As a result, the DICOM files will be potentially exchanged with other providers, without any knowledge of the risk posed by the DICOM file exchanged. The mixing of malware with Protected Health Information (PHI) will expose these HIPAA-compliant data while having the ability to compromise centralized systems of imageries. The attack was successful due to the exploitation of the preamble or the header of the DICOM image. The DICOM header, which is a 128-byte section, contains metadata and other data which facilitates compatibility between applications that are unaware of DICOM. This functionality enables the DICOM files to be viewed by non-DICOM viewers. Since the DICOM standard has identified zero courses in employing mechanisms for the detection of errors in the DICOM header, this attack has been proven to be successful.

The security leaders of DICOM, DICOM Working Group 14 (WG-14) [6] are appropriately mindful of the vulnerabilities of DICOM files and images. Despite the active participation in introducing functionalities such as secure transmission, digital signatures, and mechanisms to ensure the security of DICOM files on media and in e-mails [6], the existence of critical vulnerabilities within DICOM is readily apparent. The article [6], discusses four security attacks involving radiologic images. It has been evident that most of the attacks were successful due to the nature of the implementations of Picture Archiving and Communication System (PACS) servers with the internal hospital networks. The attacks have been noted as non-nefarious activities that were conducted as proofs-of-concept of specific DICOM vulnerabilities. Two attacks have been identified as access attacks where the security researchers were able to scan and detect numerous unprotected DICOM servers and as a result, enabled them to connect to the DICOM server from outside [6]. In 2019, deep learning was used by a security researcher to inject or remove abnormal content on MRI and CT scans, and this has been recorded as one of the data injection attacks that is possible. This was done during the transmission of DICOM messages from the scanner to the PACS and the activity has been successful in fooling 99% of the radiologists [6]. The other injection attack identified is the attack discussed in [5]. Furthermore, injection vulnerabilities such as identity spoofing can alter the public attributes of a DICOM file [6] disrupting the functionality of the DICOM Modality Worklist service [7], where its purpose is to match the relevant attributes (patient name, patient identification, sex, etc.) of the DICOM record to the correct image.

Dr. A. Padmapriya and P. Subhasri, authors of "Authentication-based Access Control Mechanism for Ensuring Privacy of DICOM Contents in Public Cloud" presented the access control technique to improve DICOM security in their research paper. In that, they discuss the below areas related to DICOM security. They said medical content security is becoming more important because of the increased use of systems for managing medical care. They gather, retrieve, store, and distribute Electronic Health Records (EHR) thanks to healthcare management systems. EHR sharing, aids in both medical diagnosis and the development of novel drugs. Thus, a standard is required to protect the contents of the EHR and to guarantee that such contents may be accessed securely. They approved DICOM as a standard for securely exchanging medical images. Sensitive patient data is contained in EHR. The goal of that project is to share DICOM information over the public cloud while still protecting its contents using cryptographic techniques. As they mention, a crucial security measure for protecting patient information in healthcare information systems is access control. Access control will make sure that only authorized users have access to the cloud's contents. This study proposes a DICOM access control system based on authentication for EHRs. Moreover, the study proposed that the most effective method of communicating medical photos is through the encryption of DICOM material. The stuff that has been ciphered as a result of the encryption procedure is then stored in a public cloud. The outcome of that research is proving that the confidentiality of DICOM contents in healthcare information systems can be maintained with the aid of the suggested authentication-based access control method [4].

According to [1] and [8], encryption mechanisms used in DICOM are not at an acceptable level. In earlier versions of DICOM, Advanced Encryption Standard (AES)–128 was used in Electronic Code Book (ECB) mode which was vulnerable to leaking information from ciphertext (semantical security is not present). Currently, most DICOM implementations work with AES-128 bit in Cipher Block Chaining (CBC) mode which is not vulnerable to data leakage from cipher text. According to HIPAA, PHI must be encrypted with an AES of 128-bit or a higher key size.

When it comes to DICOM secure communication, the study referred to in [9] confirms DICOM communication protocols have risks and communication security must be

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 10, pp 89-96, October-2023

https://doi.org/10.47001/IRJIET/2023.710012

improved. The STARTTLS mechanism vulnerability discovered in DICOM in August 2021, which results in communication continuing in an unencrypted way, if one side of the connection does not support or refuses to do so, is evidence that DICOM requires secure encrypted communication.

III. METHODOLOGY

A) Error Detection

Error detection is a crucial aspect in DICOM imaging as PACS systems associate highly sensitive information and since communication channels of PACS systems deal with DICOM images constantly. A significant process in storing DICOM images in a database is validating the integrity of the DICOM image. During the upload of a medical image into the PACS database, it must be ensured that the content of the DICOM file has not been altered by external parties or that the file has not been corrupted by any means. An essential stage during the validation of the integrity of the DICOM file is checking the DICOM header of the file for any alterations from the original file.

In the demonstration of the solutions proposed, an open-source DICOM server called Orthanc is used to showcase the approaches that will be taken to address the limitations and restrictions that have been spotlighted in the previous section.

As highlighted in the previous sections, considering the implementational structure of Orthanc, it has numerous limitations in terms of security. One such limitation is the lack of error detection mechanisms in place within the Orthanc environment. Throughout the studies we have conducted, it was evident that integrity checking for files that are being transmitted to the DICOM database is not properly established. Thus, this section of the paper is focused on describing the related approaches taken to address these problems.

Fig. 1 represents the breakdown of the processes in error detection in terms of a diagram. It visualizes that once a DICOM image is input to the Orthanc server, the error detection/file integrity checking algorithms will verify the integrity of the content of the DICOM file. Then as the next step, the DICOM header will be analyzed separately for any errors using appropriate algorithms and finally will infer whether the DICOM file is error-free or not.

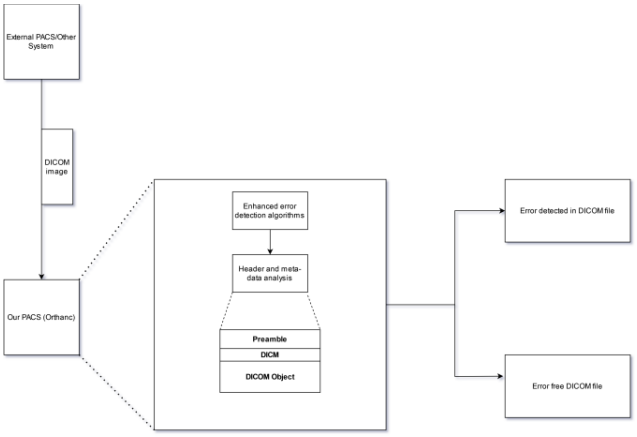

Figure 1: Implementation diagram for error detection

Through thorough analysis and studying of the specified topic, the proposed solution to address the issues includes implementing an error log to record errors, generating a Hash-based Message Authentication Code (HMAC)-based integrity checking mechanism, and introducing error detection mechanisms to the header of the DICOM file using Cyclic Redundancy Check (CRC), which was not previously available in the DICOM protocol.

1) Error log implementation

An error log is the most basic but the most essential artifact in the route to the resolution of the problem that has been identified. The basic functionality of a log is to monitor and analyze the errors that have been recognized by the potential error-checking function of the proposed solution. Log-based anomaly detection [10] plays a pivotal role in the information security industry, with its objective to identify and notify about abnormalities within a system. System administrators are the most prominent stakeholders in regard to log-based anomaly detection where they will be held responsible to manage any errors or security flaws securely. Considering a use case of the artifact, if a DICOM file is tampered with during the transmission of the file to the database of Orthanc via a man-in-the-middle attack, an error message is logged in the error log that has been implemented.

2) HMAC-based integrity checking function

HMAC is a well-known algorithm used for verifying the integrity of files and data. HMAC provides a secure and efficient approach to verifying the integrity of data using cryptographic hash functions. In the proposed approach, SHA256 is selected as the algorithm to be used for HMAC. Studies were carried out to select the best algorithm out of many possibilities for fulfilling the purpose within this context. HMAC-MD5 and HMAC-SHA1 were easily disqualified since these algorithms are known to be

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 10, pp 89-96, October-2023

https://doi.org/10.47001/IRJIET/2023.710012

vulnerable. Table I. represents the comparisons between the major contender algorithms.

Table I: Comparison of HMAC Algorithms

Algorithms	Features		
	Output size (bits)	*Performance*	*Usage*
SHA-256	256	Fast	Digital signatures, integrity checking, password hashing, etc.
SHA-512	512	Slower	Applications requiring stronger security and those which can handle the additional overhead
RIPEMD-160	160	Moderate	Used in more specific contexts where compatibility is key
Whirlpool	512	Slower	Used in specific contexts where stronger security is required

From the gathered information, it was evident that SHA-256 is the algorithm that most align with the requirements of this research since this study is focused on achieving file integrity verification with the least amount of computational overhead. The security of HMAC is dependent on the function used in it, which has proved to be secure [11] under certain assumptions. These assumptions are fulfilled by the algorithm SHA-256 which aggregates with HMAC to be a comprehensively secure hashing method.

SHA-256 algorithm functions like a one-way hash creating a digest that is shorter than the length of the message that is being hashed. Breaking the data into blocks of 512 bits (64 bytes), SHA-256 will take the blocks of data and an Initial Vector (IV) of 256 bits which is randomly chosen [11], [12]as inputs, and will generate the hash.

3) Error detection in DICOM header using CRC

Checking for abnormalities in the DICOM header is another crucial aspect of the DICOM file integrity verification process. The DICOM header includes important metadata relevant to the DICOM image and its acquisition parameters.

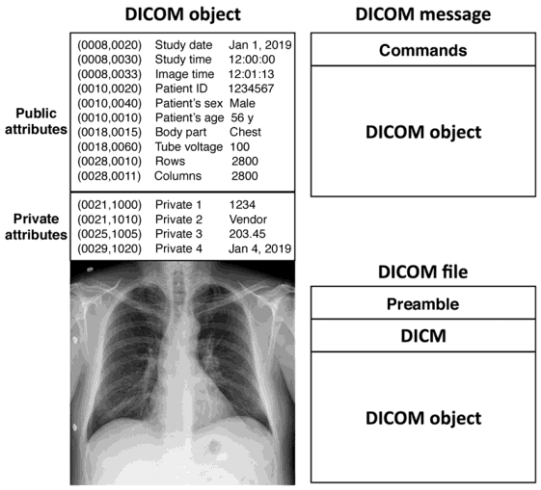

Figure 1: DICOM header

When the headers of DICOM files go unchecked in the databases of Orthanc, it increases the possibility of breaches and compromises of PACS systems via potential attacks that can be conducted through the manipulation of data in the DICOM header. One such scenario about malware attached to the DICOM header has been discussed in the previous section as well. Implementing an error detection mechanism aims to identify any errors that occur during the transmission and storage of a DICOM image in the Orthanc database.

From a wide range of error detection algorithms such as checksum, hamming code, BCH code, parity check, etc, the CRC algorithm was selected as the ideal function for this case considering multiple factors. BCH code and hamming code algorithms are not just error detection codes, but they incorporate error correction as well. This functionality, while being unnecessary, creates additional computational costs. The most important factor is that an error detection mechanism is required to preserve the integrity of the DICOM header. However, incorporating error correction algorithms will change the metadata in the DICOM header during their attempts of rectifying the errors. Thus, CRC is selected as the ideal option in this case due to its robustness in error checking. CRC algorithms provide a high level of error detection capability by being able to identify a wide range of errors such as random errors, burst errors, etc. which in some cases other algorithms fail to identify. CRC algorithms are used in many applications such as in communication services to detect errors in transmitted frames [13].

B) Access Control

To enhance the access control mechanisms of the DICOM standard, several tasks need to be accomplished. One aspect that needs to be considered is the interoperability issues with other systems within the network. The access control system needs to be designed in such a way that it is

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 10, pp 89-96, October-2023

https://doi.org/10.47001/IRJIET/2023.710012

compatible with other systems within the healthcare network, without compromising its security. Additionally, the access control system should be able to handle a variety of access control models such as Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and discretionary access control to cater to different healthcare scenarios. To demonstrate an integrated solution, access control features can be embedded into the DICOM standard itself. This will help to ensure that all DICOM implementations adhere to a common set of access control standards, making it easier for developers to build secure DICOM applications. The integrated solution will provide a more streamlined approach to access control, making it easier for healthcare organizations to secure their medical data.

The DICOM standard mainly uses RBAC. RBAC is a widely-used access control model that allows access decisions to be based on the roles and responsibilities of users within an organization. In the context of DICOM, RBAC allows administrators to define different roles or groups of users (e.g., radiologists, technicians, nurses) and to assign different levels of access privileges to each role[14], [16].

1) Lack of granularity

The RBAC model in DICOM typically relies on roles such as physician, radiologist, or administrator. However, certain situations demand more fine-grained access control based on specific attributes of the data such as patient demographics or image modality. To address this issue, DICOM should consider incorporating ABAC mechanisms, allowing for more precise control over data access based on specific attributes.

2) Static roles

RBAC traditionally assigns static roles to users, which may not accurately reflect changes in job responsibilities or organizational structure. This can result in users having more access privileges than necessary or being denied access to critical data. To mitigate this concern, a dynamic RBAC model should be implemented, where access rights are automatically adjusted based on changes in job roles or organizational structure. This could be facilitated through integration with identity management systems that regularly update user roles and permissions.

3) Inappropriate delegation

RBAC in DICOM does not inherently address the issue of inappropriate delegation, where users delegate their access rights to unauthorized individuals. Implementing stricter controls and policies around delegation is essential. This can be achieved by enforcing multi-factor authentication for critical actions, regularly reviewing access logs to identify suspicious patterns, and ensuring accountability for delegated access through user activity monitoring.

4) Lack of audit trails

The current RBAC model in DICOM may not provide comprehensive audit trails, limiting the ability to identify security breaches or instances of data misuse. To enhance security and accountability, DICOM should enhance its audit trail capabilities. This involves capturing detailed information such as user ID, date/time stamps, and the type of action performed during access and usage of data. Incorporating robust logging mechanisms and implementing advanced analytics tools can aid in proactive detection of security incidents.

C) Authentication and Authorization

Like in many other applications, authentication and authorization are critical security features in DICOM. There are numerous limitations within the context of authentication and authorization in current PACS implementations. The decentralized manner of current DICOM servers facilitates intruders to easily compromise PACS systems. Having one authentication model in use makes DICOM servers vulnerable to brute-force attacks. To address such issues, below discussed are some recommendations to remediate the challenges.

1) Certificate-based authentication

The users of the system get an X.509 digital certificate when registering to the system. The certificate provides all the information about the user, user permission levels, expiry date, and public key information. After a user inserts the digital certificate, the authentication system checks the information with the Certificate Authority (CA). When the certificate gets verified by the CA, the system creates a token with the compulsory information which is then sent to the Active Directory to request the usernames and passwords for password-based authentication.

Lack of mutual authentication creates a great threat to the users. If the users are incapable of validating the server before providing the security credentials and user information, they could be potentially feeding access information to an attacker. In the proposed system, the client requires the server's digital certificate before initializing the communication between the client and the server for password authentication.

2) Password-based authentication

User authentication needs to be verified with different types of methods to confirm the user's real identity. The proposed solution uses an LDAP server and Active Directories will be

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 10, pp 89-96, October-2023

https://doi.org/10.47001/IRJIET/2023.710012

used inside the LDAP server for authentication. Considering the main features of Active Directories[17] it enables more secure means of authenticating to the server.

Below mentioned practices are followed to enhance the security of the authentication process,

- SSL/TLS encryption for LDAP requests and responses.
- Using SHA-256 hashing for storing passwords.
- Maintaining logs for directory accesses, authentication records, and auditing for anomalies.

Once authentication is successful, the system gets all the access policies and rights available for the user with the user information in the encrypted version. All the information is encrypted by the public key of the digital certificate and the information will be checked with the certificate to validate.

3) Maintaining authentication logs

The authentication-related activities need to be available for audits whenever needed. But the Orthanc server does not contain authentication logs as audit trails. So the proposed system stores records of both successful and unsuccessful authentication requests with mandatory data.

D) Encryption

Since encryption is the primary method used by DICOM to protect the confidentiality of PHI, it can be regarded as one of the determining factors of DICOM data security. The success of the confidentiality of DICOM data depends on the encryption of DICOM data at rest and the encryption of DICOM data during transmission.

1) Encryption of DICOM data at rest

When selecting a suitable encryption algorithm to encrypt DICOM data at rest in Orthanc, and to comply with HIPAA regulations, any algorithm that can handle a key size of 128 bits or above can be used. Time to encrypt/decrypt and performance change with different encryption modes are indexes that are being used to select the optimal encryption algorithm that is suitable for the application. Due to the different characteristics of encryption algorithms, they cannot perform well in every scenario.

Research show that the Blow fish algorithm is the fastest in both encryption and decryption in the CBC mode[18].But when selecting the ideal algorithm, AES and 3DES algorithms are having the advantage over Blowfish due to excellent security and wide usage. The security of these two algorithms has been proven by various tests. Speeds of both encryption and decryption of AES-128 are greater than 3DES by a large margin. By considering the modern computing power, the median size of a DICOM file, and for enhanced encryption, AES algorithm in CBC mode with 256 bits key size is selected to encrypt DICOM data at rest.

Without proper key management, using AES-256 is pointless.

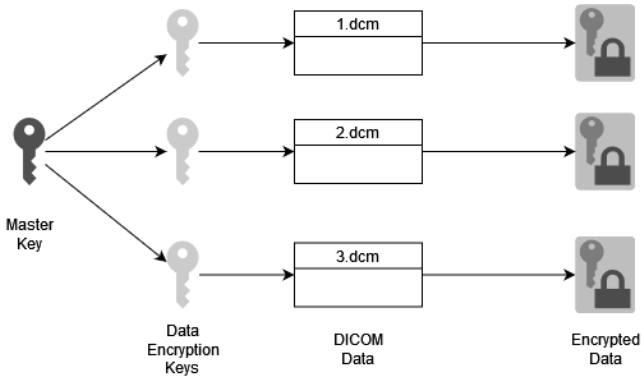

Figure 2: Comparison of encryption algorithms

To accomplish proper key management, all data encryption keys are encrypted using a master key. Each DICOM data file has a unique data encryption key that is used to encrypt and decrypt the corresponding DICOM data file.

2) Encryption of DICOM data in transmission

The vast majority of DICOM server implementations, including Orthanc, utilize TCP/IP protocols for communication. To ensure the confidentiality of TCP/IP DICOM communications, SSL/TLS security features are extensively employed[19].When relying on SSL/TLS security features, there is more tendency for security breaches to happen. The recent STARTTLS vulnerability is an example of such an occurrence. By initiating secure IPsec communications between endpoints, it is possible to add an additional layer of security to DICOM communications. IPsec tunneling provides complete encryption for packets transmitting through the tunnel. Most Next-generation firewalls (NGFW) support AES256 bits encryption in IPsec tunnels.AES-256 can therefore be used to encrypt both DICOM data at rest and DICOM data in transmission.

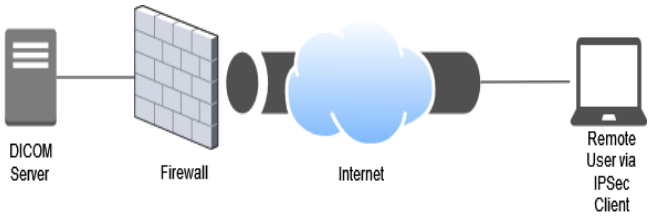

Figure 4: Secure IPSec remote connection

Using an NGFW and a corresponding IPSec client, a remote user can securely access DICOM data.

ISSN (online): 2581-3048
Volume 7, Issue 10, pp 89-96, October-2023
https://doi.org/10.47001/IRJIET/2023.710012

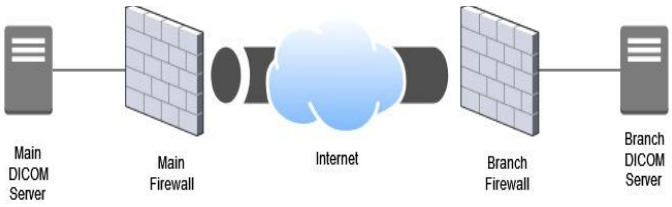

Fig. 5Secure IPSecbranch connection

Using two NGFWs, two branches can be connected securely using an IPSec connection.

IV. FUTURE WORK

Error log implementation is a significant artifact in the process of providing answers to the research gaps that have been identified. The error log plays a massive role in each of the four security components that have been discussed in the paper. However, within the context of this study, anomaly detection has been conducted through manual analysis of the generated log reports. To increase factors such as productivity and efficiency, techniques like log parsing can be incorporated into future alterations or enhancements of the solution. Log parsing converts the logs generated into a machine-readable format allowing the computer to rearrange and organize the logs into a form that allows them to be analyzed more clearly enabling system administrators to gain insights into the systems and identify potential security incidents through alerts generated by computer programs itself.

V. CONCLUSION AND DISCUSSION

In this paper, the improvement of error detection, encryption, access control, authentication, and authorization of the medical imaging protocol, "DICOM", is outlined to properly maintain the security requirements of PHI. Implementation of error logs, HMAC-based integrity checks, and CRC-based error detection in the DICOM header will enhance error detection procedures. With AES-256, effective key management, and IPsec implementation, encryption is being strengthened. Implementing ABAC mechanisms, dynamic role assignment, delegation controls, and comprehensive audit trails address challenges associated with access control procedures. Finally, implementing certificate-based and password-based authentication, along with the maintenance of authentication records, patch security holes in authentication. Although cybersecurity incidents cannot be completely prevented, the security of DICOM is strengthened by bolstering the four security components of DICOM discussed throughout. These innovations assure the confidentiality, availability, and integrity of medical data, paving the way for safer and more effective healthcare practices.

REFERENCES

[1] H. Tachibana, M. Omatsu, K. Higuchi, and T. Umeda, "Design and development of a secure DICOM-Network Attached Server," *Comput. Methods Programs Biomed.*, vol. 81, no. 3, pp. 197–202, Mar. 2006, doi: 10.1016/j.cmpb.2005.11.015.

[2] D. Peck, "Digital Imaging and Communications in Medicine (DICOM): A Practical Introduction and Survival Guide," *J. Nucl. Med.*, vol. 50, no. 8, pp. 1384–1384, Aug. 2009, doi: 10.2967/jnumed.109.064592.

[3] H. K. Huang and H. K. Huang, *PACS and imaging informatics: basic principles and applications*, 2nd ed. Hoboken, N.J: Wiley-Liss, 2004.

[4] P. Subhasri and D. A. Padmapriya, "Authentication based Access Control mechanism for Ensuring Privacy of DICOM contents in Public Cloud," *Aust. J. Basic Appl. Sci.*, 2017.

[5] Health IT Security, "DICOM Flaw Enables Malware to Hide Behind Medical Images," *HealthITSecurity*, Apr. 18, 2019. https://healthitsecurity.com/news/dicom-flaw-enables-malware-to-hide-behind-medical-images (accessed Jun. 24, 2023).

[6] B. Desjardins *et al.*, "DICOM Images Have Been Hacked! Now What?," *Am. J. Roentgenol.*, vol. 214, no. 4, pp. 727–735, Apr. 2020, doi: 10.2214/AJR.19.21958.

[7] P. M. Kuzmak and R. E. Dayhoff, "Minimizing Digital Imaging and Communications in Medicine (DICOM) Modality Worklist patient/study selection errors," *J. Digit. Imaging*, vol. 14, no. S1, pp. 153–157, Jun. 2001, doi: 10.1007/BF03190323.

[8] M. Dzwonkowski and R. Rykaczewski, "Secure Quaternion Feistel Cipher for DICOM Images," *IEEE Trans. Image Process.*, vol. 28, no. 1, pp. 371–380, Jan. 2019, doi: 10.1109/TIP.2018.2868388.

[9] Z. Wang, Q. Li, Y. Wang, B. Liu, J. Zhang, and Q. Liu, "Medical Protocol Security: DICOM Vulnerability Mining Based on Fuzzing Technology," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, London United Kingdom: ACM, Nov. 2019, pp. 2549–2551. doi: 10.1145/3319535.3363253.

[10] V.-H. Le and H. Zhang, "Log-based Anomaly Detection Without Log Parsing," in *2021 36th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, Melbourne, Australia: IEEE, Nov. 2021, pp. 492–504. doi: 10.1109/ASE51524.2021.9678773.

[11] S. Collin, "Side channel attacks against the Solo key - HMAC-SHA256 scheme," 2020.

[12] S. Gadamsetty, R. Ch, A. Ch, C. Iwendi, and T. R. Gadekallu, "Hash-Based Deep Learning Approach for Remote Sensing Satellite Imagery Detection," *Water*, vol. 14, no. 5, p. 707, Feb. 2022, doi: 10.3390/w14050707.

[13] J. Li, S. Liu, P. Reviriego, L. Xiao, and F. Lombardi, "Scheme for periodical concurrent fault detection in parallel CRC circuits," *IET Comput. Digit. Tech.*, vol. 14, no. 2, pp. 80–85, Mar. 2020, doi: 10.1049/iet-cdt.2018.5183.

[14] R. Lebre, L. Bastiao, and C. Costa, "An Accounting Mechanism for Standard Medical Imaging Services," in *2019 IEEE 6th Portuguese Meeting on Bioengineering (ENBENG)*, Lisbon, Portugal: IEEE, Feb. 2019, pp. 1–4. doi: 10.1109/ENBENG.2019.8692545.

[15] R. Lebre, L. B. Silva, and C. Costa, "A Cloud-Ready Architecture for Shared Medical Imaging Repository," *J. Digit. Imaging*, vol. 33, no. 6, pp. 1487–1498, Dec. 2020, doi: 10.1007/s10278-020-00373-7.

[16] G. Kang and Y.-G. Kim, "Secure Collaborative Platform for Health Care Research in an Open Environment: Perspective on Accountability in Access Control," *J. Med. Internet Res.*, vol. 24, no. 10, p. e37978, Oct. 2022, doi: 10.2196/37978.

[17] H. Wang and C. Gong, "Design and Implementation of Unified Identity Authentication Service Based on AD," in *2016 8th International Conference on Computational Intelligence and*

ISSN (online): 2581-3048
Volume 7, Issue 10, pp 89-96, October-2023
https://doi.org/10.47001/IRJIET/2023.710012

Communication Networks (CICN), Tehri, India: IEEE, Dec. 2016, pp. 394–398. doi: 10.1109/CICN.2016.84.

[18] N. Alanizy, A. Alanizy, N. Baghoza, M. AlGhamdi, and A. Gutub, "3-LAYER PC TEXT SECURITYVIA COMBININGCOMPRESSION, AES CRYPTOGRAPHY2LSB IMAGE STEGANOGRAPHY," *J. Res. Eng. Appl. Sci.*, vol. 03, no. 04, pp. 118–124, Oct. 2018, doi: 10.46565/jreas.2018.v03i04.001.

[19] J. Zhang, "DICOM Image Secure Communication with Internet Protocols," in *Teleradiology*, S. Kumar and E. A. Krupinski, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 33–47. doi: 10.1007/978-3-540-78871-3_4.

Citation of this Article:

A.N. Somasundara, S.T. Jayathunge, D.M.C.P. Jayasooriya, E.M.H.O. Ekanayaka, Kanishka Yapa, Uditha Dharmakeerthi, "Ensure Security and Privacy of Medical Imaging through Secure DICOM" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 10, pp 89-96, October 2023. Article DOI https://doi.org/10.47001/IRJIET/2023.710012

****

