National Conference on Engineering Innovations and Solutions (NCEIS – 2018)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 6 | ISSN : 2456-3307

A Survey on Secure DICOM Transfer through Network

Divyashree R*, Dr. S Kuzhalvaimozhi
Information Science and Engineering, The National Institute of Engineering, Mysuru, Karnataka, India

ABSTRACT

DICOM, a standard used for secure connection and transfer of digital images, which is the integration of medical images with patient related information. The procedures in hospitals require the radiological images which contains few attributes of the image and the patients whose information belongs to. Report without any images is difficult to understand by common man, hence it requires a combination of both image and report. The main issue during transfer of these images is their security. It must be taken care that transfer of data should be protected from third parties, for this DICOM should provide some mechanism for security. Many methods are available for securing the data, by encrypting and decrypting the data. The developing system is used to transfer DICOM files, and extend the same in the system to meet the requirement of security. There are hospitals which allow systems to connect to hospital infrastructure only via secure way i.e., certificate based authentication. The current system on which it is being used supports only standard DICOM protocols, hence the systems cannot be used in hospitals which mandates certificate based authentication. Therefore, the systems which supports certificate based DICOM connectivity software is being developed and this has become a vast area for research.

Keywords: DICOM, Certificate, PACS, Security

I. INTRODUCTION

Storage formats standardization is a very important requirement to enable proper operations between devices and equipment within Healthcare system. Digital Imaging and Communications in Medicine (DICOM) being the most widespread and accepted standard for effective, efficient and secure medical imaging storage and transfer over large geographical areas.

DICOM is the healthcare industry standard for transfer of digital medical images and other medical information between different systems such as computers. Since various modalities such as CT, MR, XA and US are based on this DICOM standard, digital treatment is possible. The dynamic process of the examining position of patients is reflected by multiple frame images that exist in DICOM medical images. The commonly used image processing software cannot process, display and convert this file format because of the particularity of the DICOM image format.

DICOM makes medical image exchange more easy and independent of the imaging equipment manufacturer. Besides the image data, DICOM file format supports other information useful to describe the image. This makes DICOM easy to use and the data exchange fast.

In order to efficiently manage the storage capacity of PACS, DICOM allows image compression, JPEG2000 is one of the most used compression algorithm in

DICOM images due to its compression efficiency. A highly secure role-based access control policy has been implemented by DICOM. The security policy is entirely based on cryptography; the most sensitive DICOM contents which are fields and/or the image if it identifies the patient are put into individual digital envelopes and sealed by means of Cryptographic Message Syntax (CMS). With current security measures, a corrupted DICOM file can still be queried and the contents of non-corrupted envelopes can be retrieved normally. many times certain sensitive information associated with the image is engraved on the frame itself. DICOM supports anonymization which is by blackening the data on the image, it does not define specific mechanisms for finding

DICOM provides the basis for picture archiving and communications systems (PACS) and is the most extensively used standard for storage and transmission purposes. PACS requires high-speed networks to transmit large image files between components. In case of intranet, that is, PACS within a healthcare campus, Gb/s switches with Mb/s connections to workstations are mostly adequate and is a standard in most hospital and university network infrastructures. Their transmission rates, even for large-image files, are acceptable for clinical operation. However, in case of using the Internet for tele radiology applications or enterprise PACS, image data must be transmitted between hospitals and campuses. While transmitting these images from hospital repository to PACS or vice versa, confidentiality of data place an important role.

Thus, although the information can be protected in the DICOM header, the same information is sometimes accessible in the frame. The data which faces such problem usually is the patient's name, which many times is displayed in the frame which is also included in the DICOM header. To overcome this problem, a file format enabling the segmentation of frames in different regions in combination with signal-based security methods that enhances the protection of the information can be used.

II. LITERATURE SURVEY

DICOM makes medical image exchange more easy and independent of the imaging equipment manufacturer. Besides the image data, DICOM file format supports other information useful to describe the image. This makes DICOM easy to use and the data exchange fast.

DICOM file structure:

The structural units of DICOM file DICOM sets, these DICOOM image files are based on standard DICOM. The DICOM sets consists of data elements which are in particular order. An example of DICOM structure which consist of DICOM file header and DICOM data sets is as shown in the Figure1.

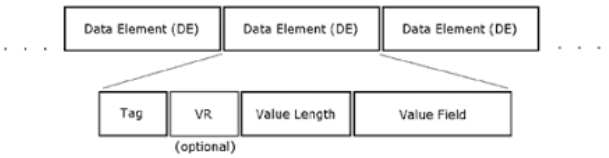

Figure 1. Structure of DICOM

DICOM file header:

The 128 bytes in the DICOM file header is known as DICOM preamble which is used for providing compatibility with the format of common file. The information required for identifying the DICOM data set is present in the DICOM file header. If the 4 bytes behind DICOM preamble consists of "DICM", then the file is based on DICOM standard otherwise not.

DICOM Data Set:

The data set is formed by the most basic unit called data elements. Each data element consists of 4 parts, they are tag, value representation (VR), value length (VL) and value. The data elements are arranged in tag order. Each tag has 16 bits of unsigned integer where first 8 bits represent group number and the second 8 bits represent element number. All the data

elements are uniquely identified by the tag. The data type of the data element is specified by VR and it must exist if transfer syntax is explicit. It can be ignored if it is implicit.

Image Coding:

The most important data unit is the pixel data identified by the tag (7EE0, 0010) is the pixel data identified and is the most important data unit. It is the last element in the data set and contains useful information required for medical image display. This pixel data is required for converting single frame DICOM image to PNG and also to multiple frame DICOM image to MP4. The other important data elements are:

- ✓ The number of frames is identified by tag (0028, 0008). It is greater than 1 in case of multiple frame image.
- ✓ The height of the image (rows) is identified by tag (0028, 0010).
- ✓ The width of the image (columns) is identified by tag (0028, 0011).
- ✓ The number of bits allocated for each pixel sample (Bits Allocated) is identified by tag (0028, 0100).
- ✓ The number of bits stored for each pixel sample (Bits stored) is identified by tag (0028,0101)

DICOMDIR

DICOMDIR contains the metadata about the DICOM files. It is a special DICOM file which is like an index of DICOM files or like a small DICOM database. If present, the DICOMDIR is always present in the root folder of the media. The DICOM files contain their own DICOM data objects and DICOMDIR contains information about these DICOM files. All directory data is classified into four DICOM levels by DICOMDIR: Patient, Study, Series and Image as shown in Figure2. For each file in the DICOM folder, DICOMDIR consists of 4 entries- patient, study, series and image information corresponding to that file.

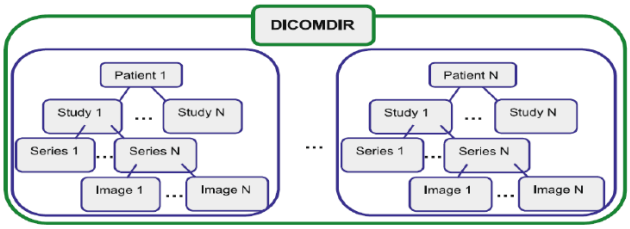

Figure 2. Structure of DICOMDIR

III. SECURITY ISSUES

Security plays an important role while transferring the medical images through different network. Security components include Confidentiality, privacy, integrity, authenticity. High security is required as the medical images contain the sensitive information of patients. When transferring the medical images through network, the security threats are as follows:

Confidentiality:

Confidentiality is considered as important for following reasons. It builds and develops trust. It helps in free flow of information between the client and server and acknowledges that a client's personal life and all the issues and problems that belongs to them.

Privacy:

Privacy is the process of maintaining the security and confidentiality of patient records. It includes both the conversational data by health care providers and the security of medical records. This can also refer to the physical privacy of patients from other patients and providers while in a medical facility.

Integrity:

Integrity means ensuring that the image captured or provided is the original or first handed information and it has not been corrupted. Since many participants are involved in the network based medical image exchange, any modification can take place due to the participants knowingly or

unknowingly. Hence integrity is a big issue to medical images in network.

Authenticity:

The medical images can be transferred only if the patients and doctors is authorized. For authenticity, the identity of the client and the server must match with each other. If the details are revealed, unauthorized users can have access to the data.

IV. SECURE DICOM COMMUNICATION

Secure transmission of data from one hospital to another through public networks is usually characterized in terms of privacy, authenticity, and integrity. Figure3 shows a data flow of image secure delivering from one hospital to another through the network.

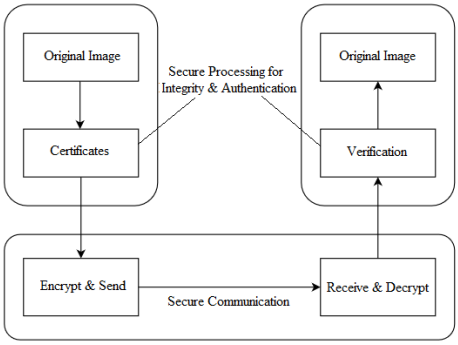

Figure 3. Data flow of medical image secure communication from one site to another through network

The two processing steps to provide secure measures for delivering images: First, for the data integrity and authenticity, the hash computing on data and digital signature. It also includes the decoding signature and comparing digest, on the images before and after transferring at both the sending and the receiving sides; Second, for the privacy of the data, the secured communication channels are provided to transmit the image through networks. The focus is on the secure measure, where data privacy, with evaluation results are given more importance. There are two methods to provide secure communication channels with TCP/IP protocols: IPSec and SSL/TLS.

Medical image communication uses DICOM communication services to transfer the image data between the imaging modalities such as PACS archiving server, workstations, and other components. It also includes transfer between tele radiology systems, and in enterprise PACS environment with WAN interconnection. In DICOM, the open system interconnection (OSI) reference model is used for the interconnection of medical-imaging equipment, as shown in Figure4. DICOM uses the OSI upper-layer service to separate the exchange of DICOM messages at the application layer from the communication support provided by the lower layers. For the medical-image transmission through high speed broadband networks with IPv4, the DICOM upper layer for TCP/IPv4 must be developed and also make it compatible with IPv4. For software, it only needs to replace the original TCP/IPv4 socket functions with requests for RFC standard TCP/IPv4 compatible socket functions, provided by each operating system, recompile the software, and link it to DICOM services. For this environment, there is a need to install the IPv4-stack software and perform some re-configurations, such as assigning IP address, configure the tunnel for that specific operating system, such as Windows XP, which have already supported the IPv4.

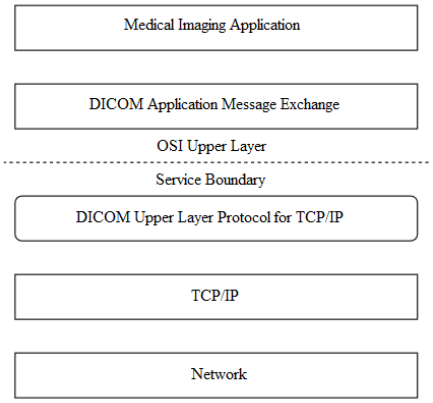

Figure 4. DICOM network communication protocols architecture.

For this, we come up with three basic IPv4-enabled DI-COM-communication services and applications:

1. DICOM Storage (C-Store) service-class user (SCU)) and service-class provider (SCP);

2. DICOM Query (C-Find) SCU and SCP;
3. DICOM Retrieval (C-Move) SCU and SCP.

DICOM provides a standardized method for ensuring secure communication and certificate based verification. The secure communication of IPv4 enables DICOM image transmission and it utilizes IPsec protocol, which is now used in virtual private network (VPN)) applications, and will be widely used in high-speed broadband networks.

The SSL was developed by Netscape Communications which allows secure access of a browser to a Web server. SSL has become the standard for Web security. It provides secure communication channel between client and server by providing mutual authentication. Authentication uses certificates for integrity, and encryption for privacy. The protocol was designed to support specific algorithms used for cryptography, digests, and signatures. SSL 3.0 is the basis for the TLS protocol, which is still in developing stage by the Internet engineering task force (IETF).

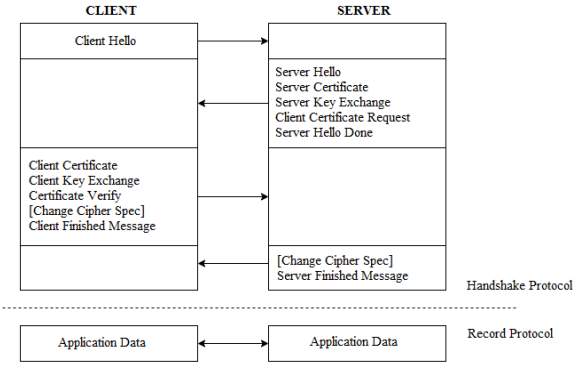

Figure 5. SSL Handshake between Client and Server

The SSL protocol supports both public-key and symmetric-key encryption. Symmetric-key encryption is faster than public-key encryption, but public-key encryption has better authentication techniques. SSL consists of two protocols: the handshake protocol and the SSL-record protocol. The handshake protocol gives information on how the peer entities exchange associated information, such as, SSL version and ciphers, and authenticates certificate. The SSL-record protocol gives the format of SSL record, in which all of the SSL-associated messages should be transferred. The SSL connection is executed in two phases: the first is the handshake, and the second is data transfer as shown in the Figure5. The data flow of the DICOM Storage includes SCU and SCP entities with SSL/TLS support. The SSL/TLS works between the TCP layer and the application layer. For IPSec and SSL/TLS-based security communications, X.509 certificates were created for both sites of DICOM C-Store SCU and DICOM C-Store SCP from the same certificate authority attached in the ssl tool kit. After the complete transfer of the images the ssl tool indicates the Handshake between the client and the server and finally indicating the closure of socket.

V. CONCLUSION

DICOM, a standard protocol used in the transfer of digital images which is the integration of medical images with patient related data. In this paper the various security challenges faced while transferring the medical images through the network and how the medical images is transferred from client and server using certificate based authentication is discussed. Using this method, the third party or man-in-middle attack can be avoided.

VI. REFERENCES

1. J Umamaheswari, Dr. G. Radhamani, “A Hybrid Approach for Classification of DICOM Image,” World of Computer Science and Information Technology Journal , 2011
2. Jeffrey D. Robinson,”Beyond the DICOM Header:Additional Issues in De identification,” American Journal of Roentgenology, December 2014,Volume 6,Number 3
3. Overview of RSNA DICOM Demonstration [Online], (1997), Radiological Society of North America (RSNA) and Mallinck-rodt Institute of Radiology.

4. Shini S.G, Dr Tony Thomas, Chithranjan. K "Cloud Based Medical Image Exchange Security Challenges", Elsevier ,2012.
5. MAnuja and C.Jeyamala "A Survey on Security Issues and Solutions for storage and exchange of medical images in cloud", International Journal of Emerging Trends in Electrical and Electronics (IJETEE – ISSN: 2320-9569) Vol. 11, Issue. 6, October-2015.
6. Rescorla E. (2001) SSL and TLS: Designing and Building Secure Systems.
7. Mahmoud Ismail,James Philbin," Fast processing of digital imaging and communications in medicine (DICOM) metadata using multi series DICOM format," Journal of Medical Imaging ,(Apr–Jun 2015).
8. Arcangelo Castiglione et.al, "Cloud-based adaptive compression and secure management services for 3D healthcare data", Future Generation Computer Systems, Elsevier,2014
9. JB. Lima , F.Madeiro , F.J.R.Sales ," Encryption of medical images based on the cosine number transform", Elsevier, 2015
10. DICOM, https://www.leadtools.com/sdk/medical/dicomspe
11. https://en.wikipedia.org/wiki/