AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

Authentication based Access Control mechanism for Ensuring Privacy of DICOM contents in Public Cloud

[1]P. Subhasri and [2]Dr.A. Padmapriya

[1]*Ph.D Research Scholar, Department of Computer Science, Alagappa University, Karaikudi – 630 004, Tamilnadu, India.*
[2]*Associate Professor, Department of Computer Science, Alagappa University, Karaikudi – 630 004, Tamilnadu, India.*

Address For Correspondence:
Ph.D Research Scholar., Department of Computer Science., Alagappa University, Karaikudi – 630 004, Tamil Nadu, India. +91 741 842 8638, E-mail: swarnasubha91@gmail.com

ARTICLE INFO

Article history:
Received 28 May 2017
Accepted 22 July 2017
Available online 26 July 2017

Keywords:
Access Control, Electronic Health Records, DICOM contents, Authentication.

ABSTRACT

Background: The extended use of medical healthcare management systems is increasing the need for medical contents security. Because the healthcare management systems allow us to collect, extract, store and share the Electronic Health Records (EHR). Sharing of EHR helps in medical diagnosis as well as assists in inventing new medicine. Therefore a standard is needed to secure the EHR contents and to ensure the access of those contents. DICOM is a standard for sharing medical images in a secured way. **Objective:** Electronic Health Records contains sensitive data of the patient information. This research work focuses on securing the DICOM contents using cryptographic methods and sharing them over public cloud. Access control is a fundamental security barrier for securing the patient details in healthcare information systems. Access control will ensure whether the contents of the cloud are accessed by authorised person or not. **Results:** In this paper, an authentication based access control mechanism for EHR-based DICOM (Digital Imaging and Communications in Medicine) is proposed. DICOM is the file which contains both patient image details as well as patient data. The encryption of the DICOM content is the efficient way of sharing medical images. After the encryption process, the resultant ciphered content is stored in public cloud. **Conclusion:** With the help of the proposed authentication based access control mechanism, the confidentiality of DICOM contents can be preserved in healthcare information systems.

INTRODUCTION

The enormous increase in medical records is a big challenge in health care sector because of the complexity involved managing, storing and processing these records. The unstable escalation in the amount of medical contents is due to factors such as increasing the patient population, new medical imaging technologies such as 3D imaging, PET/MR scans (NEMA, 2003). Most of the medical organizations do not have much IT resources or storage for managing the increasing volume of data (Deepak and Manjunath, 2015). Medical records sharing enable to share the records/content across all healthcare stakeholders, starting with public hospitals and progressively to healthcare establishments in the private sectors (Suhaila Mohammed *et al*., 2017) with the quick and accurate access to essential medical information. The main advantages are, it improves the quality of care provided and helps to reduce the cost for patients and doctors. Because they can now views the scan images online, thereby reducing the need of repeating the tests (Dhivya and Ramkumar, 2016).

Cloud computing is a promising solution to share the healthcare information over the internet. It is an on-demand network access to share a pool of configurable computing resources with minimum managing effort and good service provider interaction (Suresh and Kavitha, 2015). Cloud computing will helps the users in handling the healthcare information efficiently, expanding the storage capacity and providing secured access to the

To Cite This Article: P. Subhasri and Dr.A. Padmapriya., Authentication based Access Control mechanism for Ensuring Privacy of DICOM contents in Public Cloud. ***Aust. J. Basic & Appl. Sci.,*** *11(10): 128-136, 2017*

information by access control mechanisms (Srinivasan and Raja, 2016).The main objective of cloud computing is to share the data from provider to end users through the internet (Parthasarathy and Jothi, 2015).

DICOM (Digital Imaging and Communications in Medicine) is the EHR based medical content which is the universal standard for communication of medical details over networks (Wan Rozaini *et al*., 2017). The DICOM was predicted by NEMA in 1983. It has four types of security profiles namely, secure usage profiles, secure transport connection profiles, digital signature profiles, and media storage security profiles. These security profiles assure the protection of health records during its exchange process (NEMA, 2003).

The medical records exchange process permits to share the medical contents in a secured way (Balamurugan *et al*., 2015). Generally, DICOM medical contents enclosed the sensitive data about patient in its images like X-ray, MRI, CT images. Sharing of those data happens to be a biggest challenge (Hemalathadevi and Rajeswari, 2015). The intruders may attack the contents and access the confidential information about the patient. When an EHR medical record is attacked, it loses its trustworthiness (DICOM security chapter). These arises a need for sharing medical contents in a secured way.

The paper is organized as follows. Section 1 provides a general description of DIOCM medical contents and DICOM file details. Section 2 presents a brief review of the related work, Security constraints of DICOM contents sharing and the main objectives of the proposed method. Section 3 elaborates the secured storage of DIOCM content in public cloud and the overall architecture design of the process. Section 4 illustrates the results and discussions of the proposed authentication based access control mechanism. The contribution of this research work is concluded in section 5.

Background Study:

Related works:

(Rabi Prasad Padhy *et al*., 2012) proposed a cloud based model for developing a rural healthcare system. The authors also discussed the existing health care providers; they said the past providers such as the family doctors have stored their patient details on paper locally. This environment did not provide integrity and confidentiality while exchanging these details. The authors presented overall system architecture along with the functional components. They also highlighted the advantages of their proposed cloud based model.

(Chia-Chi-Teng *et al*., 2012) developed a framework for mobile medical imaging devices and applications to communicate with a cloud based image storage system in a secured manner. This paper also offers a management service system using DICOM protocol. They discussed their implementation which improves the interoperability of previously standalone and proprietary mobile devices with existing clinical systems.

(Chenghao He *et al*., 2010) proposed a cloud based hospital information sharing system which shares the information and high-end processing in the cloud. This article described the cloud based HIS that is flexible, extensible and has practicable framework for acquiring resources from the cloud. The authors stated the system will reduce the hospital operating costs and significantly improve its operating efficiency.

Security constraints in DICOM Medical content sharing:

- Lack of integrity and confidentiality.
- Excessive resources utilization due to the redundancy of medical image storage at different locations.
- Difficulty in retrieving of patient's medical history in the Natural Disaster-affected areas.
- Lack of DICOM/IHE/HL7 Standards awareness and its importance among Doctors, Technicians, and PACS Administrator and Hospital staffs.

Current media storage security profile in DICOM facing some pitfalls, the major one is they are not robust against different types of attacks (http://www.dicomgrid.com/). In order to overcome this kind of drawbacks, a high-security system is proposed in this paper. The proposed system will store the DICOM content in a Trustworthy Health Information Cloud. Using cryptographic techniques, the details are stored in a secured way. Since the EHR-based DICOM information's are to be stored in the cloud, data redundancy will be eliminated (http://mgitech.wordpress.com). Access to the resources will be provided based on suitable authentication.

Objectives of the proposed work:

- To ensure individual's privacy of DICOM medical contents through cryptographic methods.
- Store the DICOM contents in a cloud there by auditing redundancy.
- To provide authentication based access to the stored DICOM contents, thereby ensuring security.

Authentication based access control for securing DICOM contents in public cloud:

This paper proposes an authentication based access control mechanism for ensuring the privacy of EHR. With the help of this access control system, the contents are accessed by authorised persons alone. The .dcm file is read using new DICOM viewer (Subhasri and Padmapriya, 2015) and split into Bmp image and tag. Both portions are encrypted using random encryption methodology, either by modified vigenere cipher or multilevel

encryption method. In modified vigenere cipher technique (Subhasri and Padmapriya, 2015), a substitution based method, the units of plaintext are replaced with cipher text by a set of key values. In this method 0-255 numbers are generated randomly throughout the processing to encrypt the DICOM contents. The modified vigenere table consists of the numbers written out 256 times in different rows, each number shifted cyclically to the left compared to the previous number, corresponding to the possible 256 numbers.

In multilevel encryption method is three step chain based processing. The first step is position based transposition. The resultant matrix is the input of the second phase which is XOR based function. The resultant matrix of this second step is the input of the advanced vigenere cipher substitution. Here the possible numbers are written out 255 times in different rows, the table rows are changed every time based on the image order is odd and even.

Proposed Architecture:

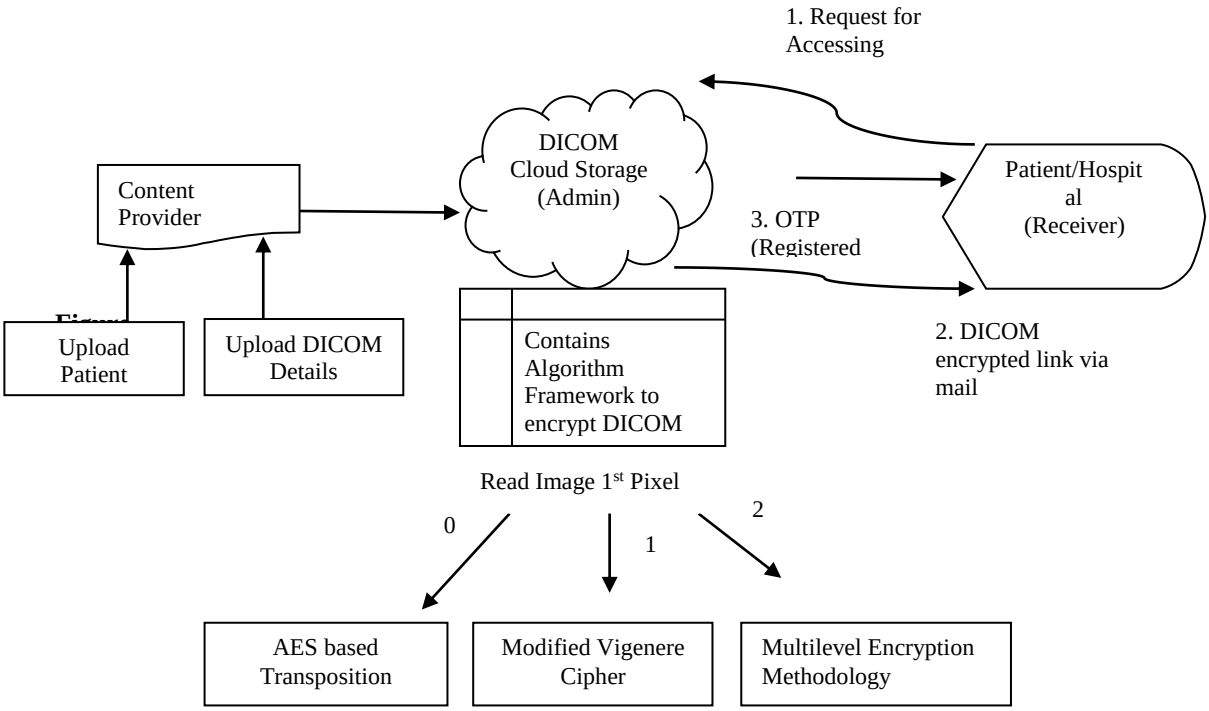

Fig. 1: Flow diagram for securing the DICOM contents in cloud with Authentication

The admin uploads the patient details and DICOM contents to the public cloud of the content provider, which are to be processed. Administrator is the DICOM controller and has the algorithm framework to encrypt/decrypt the DICOM. Whenever the encryption process is complete, the controller sends a link to the user via registered email. The receiver/user can access the content by following the steps on mail which will redirect receiver/user to the registration process. The registration is mainly to authenticate the user.

Secure Storage of DICOM content in public cloud:

The following are the steps to store the DICOM on public cloud.

Step1: The cloud DICOM controller (administrator) will add patient details into the cloud.

Step 2: The uploaded .dcm file is divided into image and tag.

***Step 3*:** The image is divided into 2*2, and get the first pixel of the image. The pixel value is divided by 3. If the remainder is 0 it will choose AES based transposition, if 1 it will choose modified vigenere cipher technique otherwise it will choose multilevel encryption methodology.

***Step 4*:** The tag also encrypted using the same procedure in step 3.

Step 5: Dicom contents are encrypted by using these above steps and stored into cloud storage region.

Step 6: By clicking sent to patient button the secured link is sent to patients registered email id. The Screen shots are shown below,

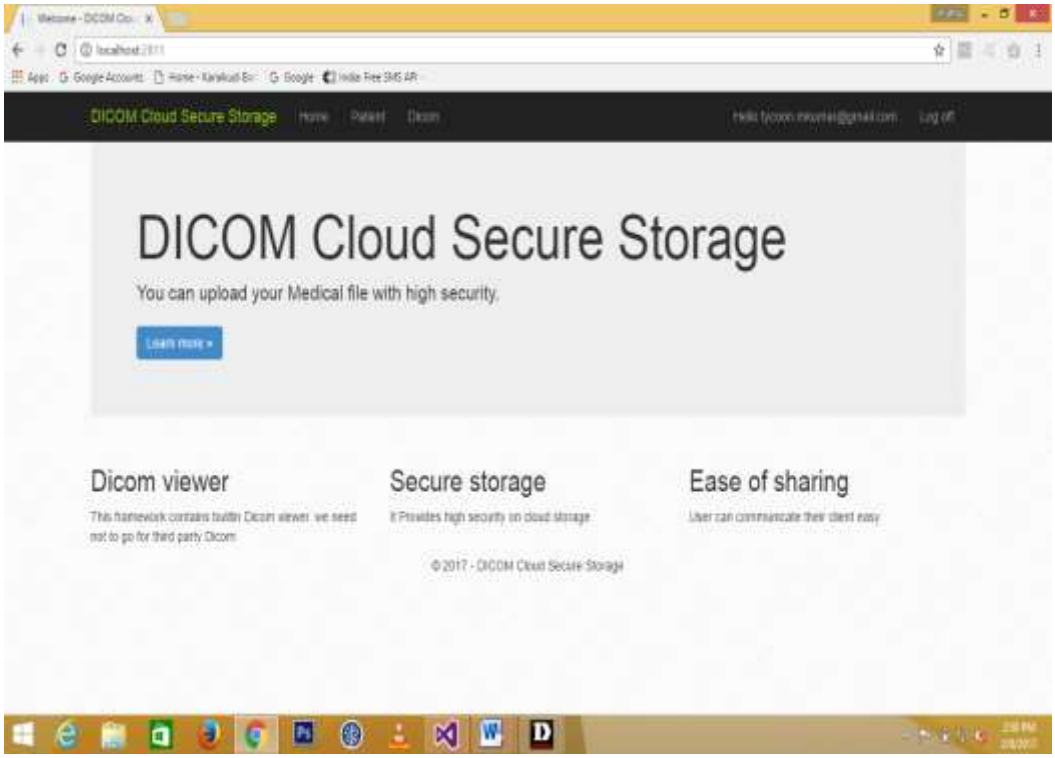

Fig. 2: Dicom cloud secure storage Application

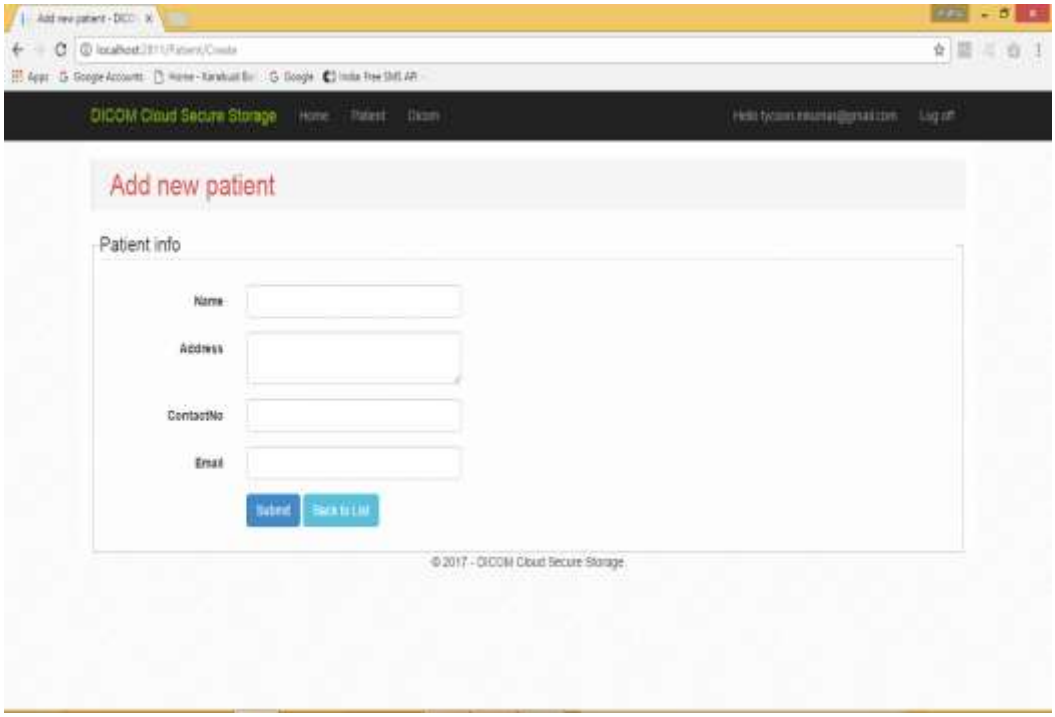

Fig. 3: Dicom cloud secure storage Add patient View

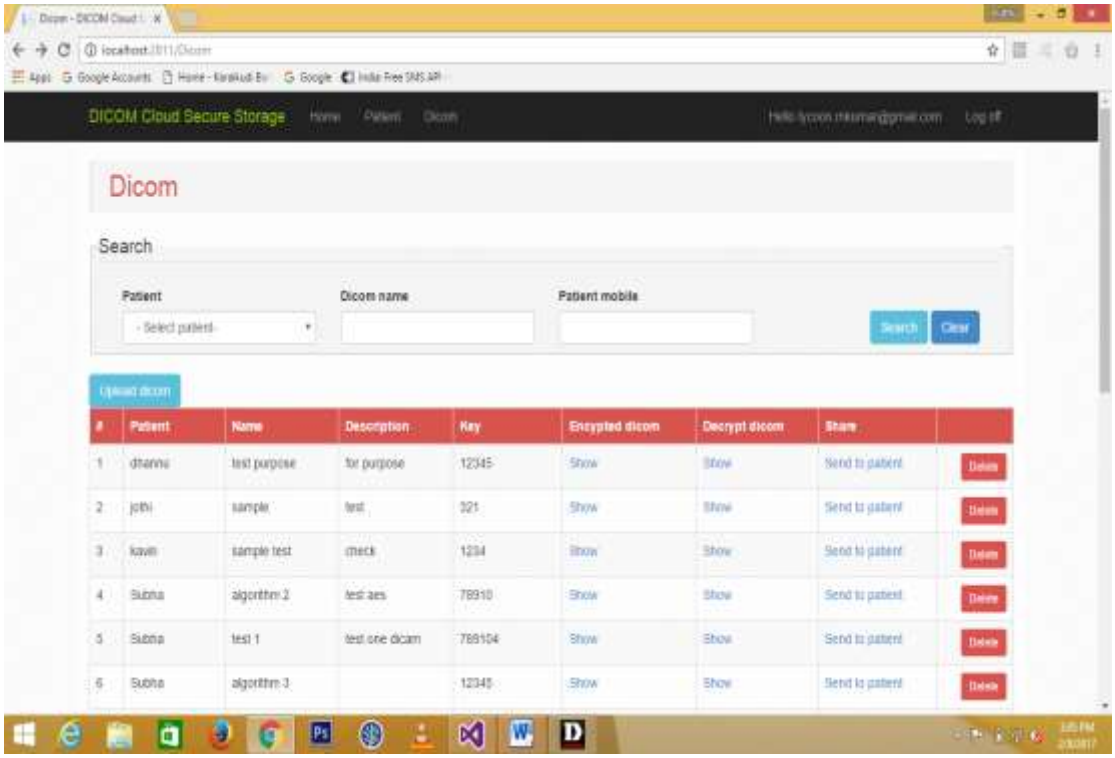

Fig. 4: Patient details added view

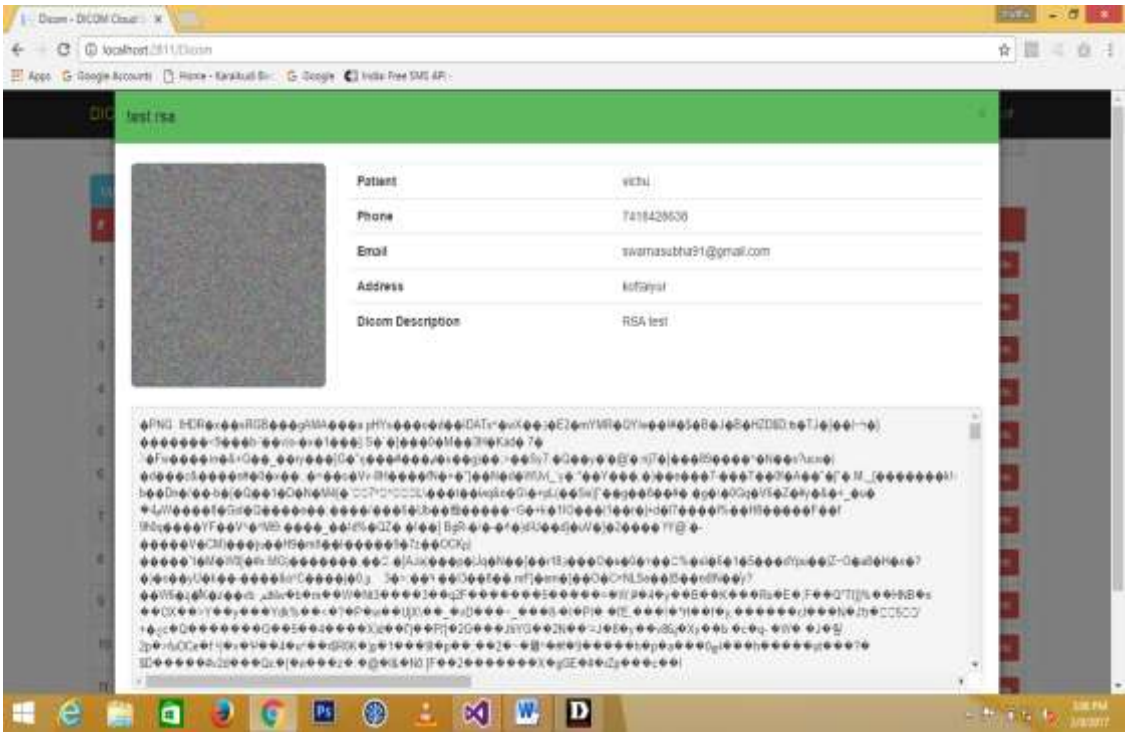

Fig. 5: Dicom cloud secure storage Encrypted view

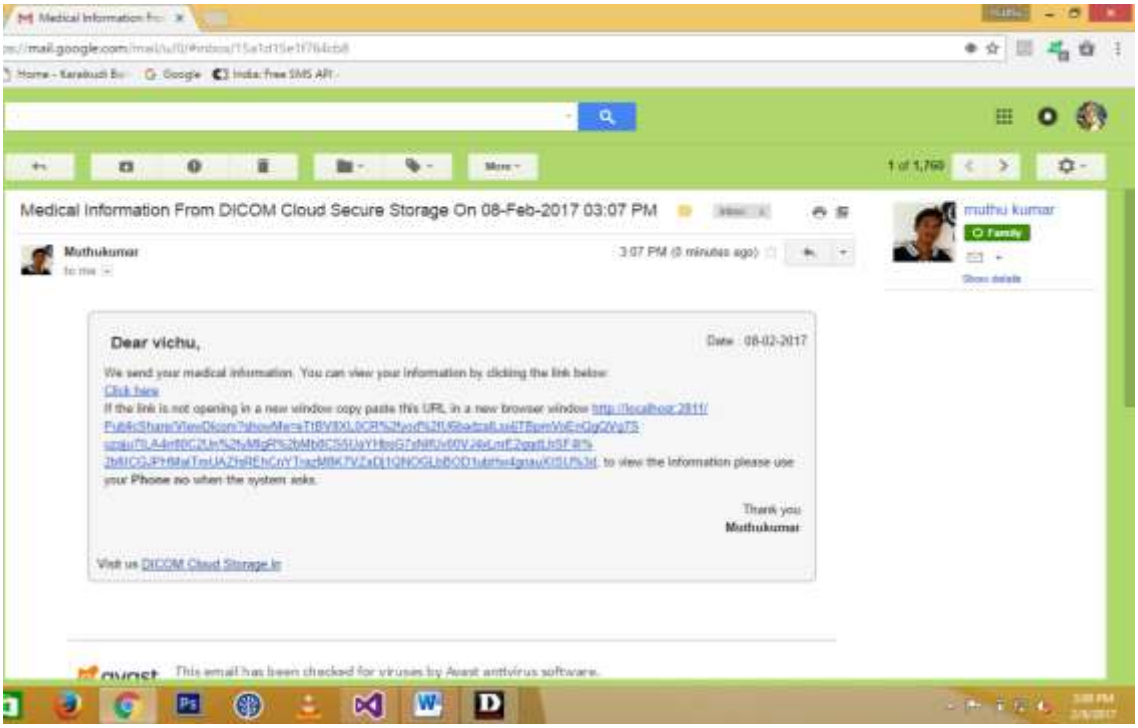

Fig. 6: Dicom accessed Authentication

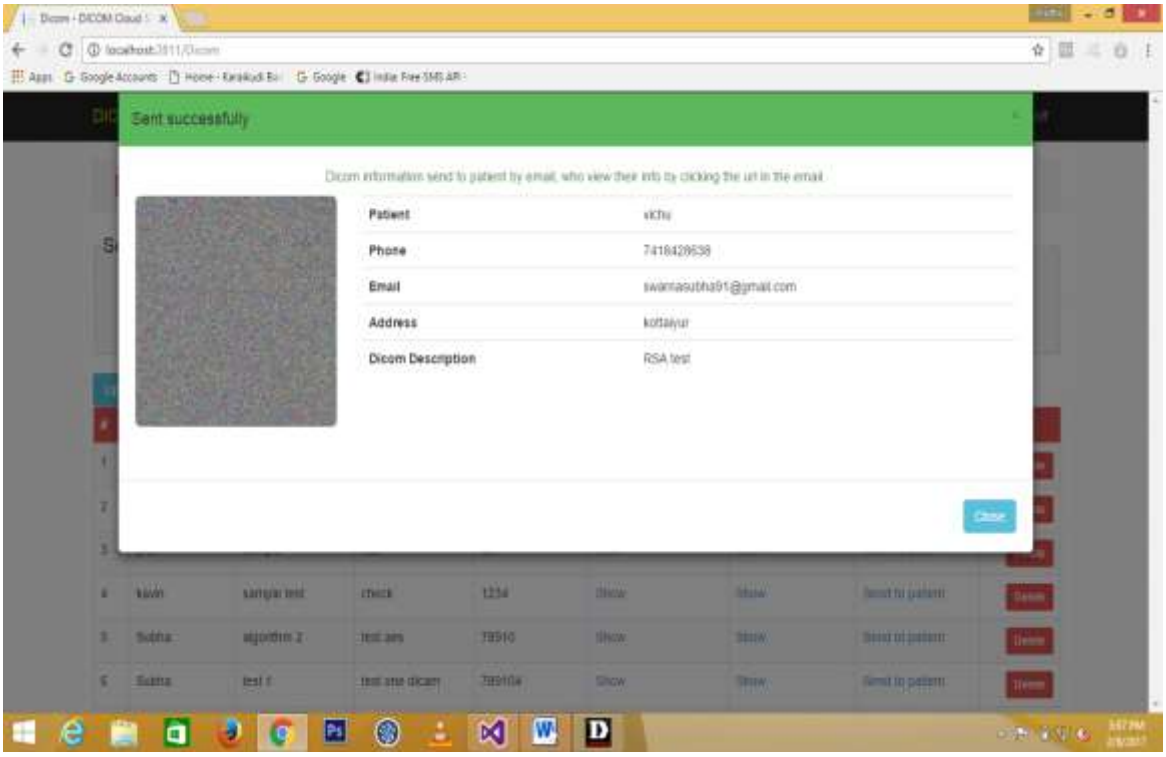

Fig. 6.1: Dicom accessed Authentication

Proposed Authentication Based Access Control Mechanism:

The proposed authentication based access control mechanism includes RSA based OTP generation to fulfill the requirements of the authorized users. When the patient wants to access their details they send an accessing request to the Dicom controller. The Dicom controller then sends a secured link to the patient's registered mail id. In addition to the secured link RSA based OTP was send by the patient's registered mobile number. RSA is the well known and widely used method that uses time based OTP to generate unique passwords.

The characteristics of this RSA based OTP used for authentication are listed below,

- The OTP is valid for a short period of the time for 5 minutes.
- It is randomly generated one.
- When the OTP is received on patient registered mobile number, the patient is authenticated to access the DICOM.

Steps for Generating OTP:

Step 1: In order to authenticate the patient, two inputs are required, 6 digits OTP and a secret key. For example the generated OTP is 891632, and a secret key is 29.

Step 2: Sometimes the hacker may guess the secret key after a series of sniffed transactions. So in this paper, a summation of secret is used. Generally, summation is the operation of adding a sequence of numbers; the result is their sum or total. Here the summation of individual digits of the OTP is considered as secret key.

Step 3: Authentication is done using OTP and summation of the secret key.

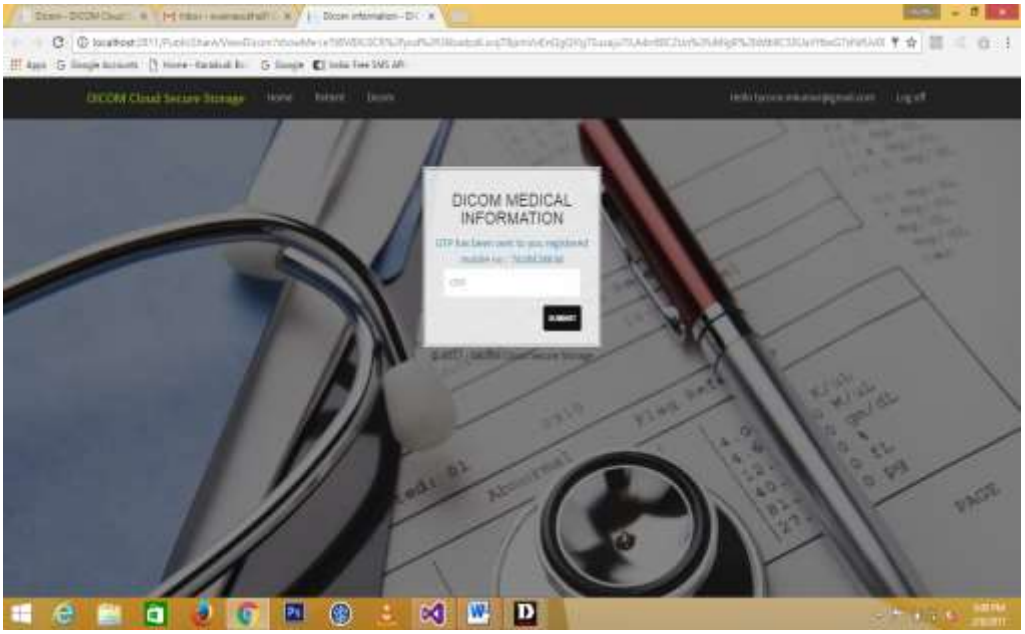

Fig. 7: Dicom Cloud Secure Storage OTP Generation

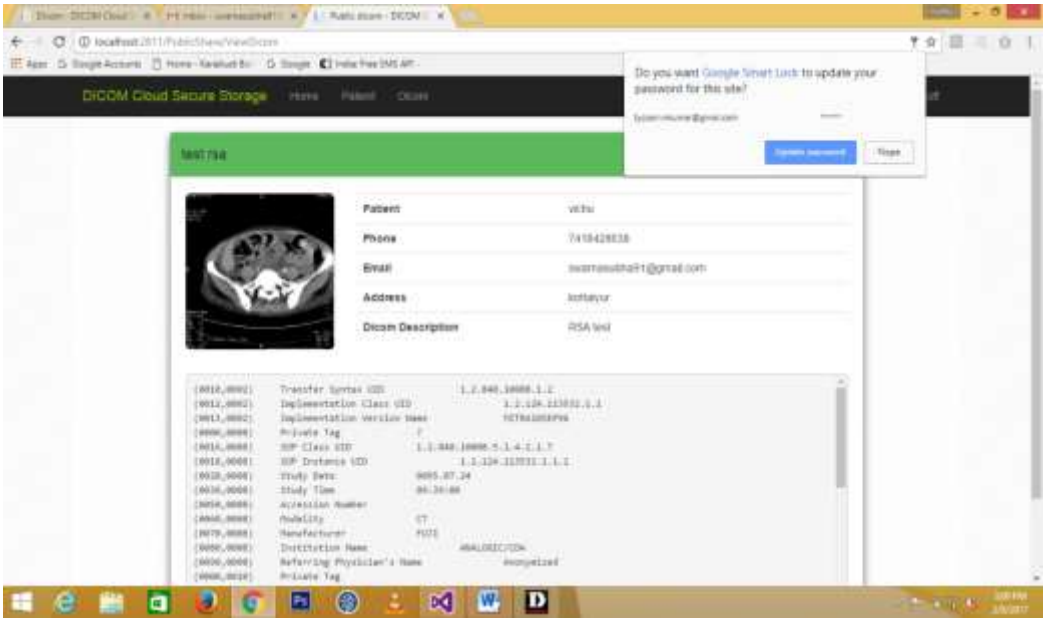

Fig. 8: Decrypted DICOM content on public cloud the user view

Conclusion:

Modern technological advances made an essential modification in the current health care systems including medical image management and Hospital information system (HIS). The evaluation of medical records management technologies offers sharing of patient details through various methods. The medical image which enclosed sensitive information about the patient particulars is shared over the network; happen to be the biggest challenge. These arises the need to protect and prevent the medical records from malicious attacks. The hackers may attack the patient details either by maintaining the sensitive data or get access to the confidential information about the patient. When an image attacked it will lose its reliability. Therefore the use of the attacked image leads to wrong treatment for the patient. Cryptographic methods are used to maintain the secrecy of medical image.

The DICOM technology is suitable when sending images between different departments within hospitals or/and other hospitals, and consultants. A DICOM file contains the patient image with the explanation details. Therefore, a single DICOM file includes a header and all of the image data. The DICOM medical contents which enclosed sensitive information about the patient particulars are shared over the network happen to be the biggest challenge.

Cloud computing offers internet based technologies on virtualized storage and telemedicine services. Cloud computing provides enormous prospects in the health care management system which characterize the efficient handling of medical records, expand storage capacity and secure level authorized transaction of the medical contents. Over cloud environment, the hospital management system processed various computer paradigms like transmission, storage and further retrieval of patient details needs on the user. While the transmissions of medical records on the cloud it has some disadvantages also, data security considered the main problem on distributed storage systems.

Cloud computing technology includes a set of important policy issues like privacy, security, anonymity, reliability, telecommunications capacity and among others. Over cloud environment the hospital management system processed various computer paradigms like transmission, storage and further retrieval of patient details needs on the user. But the important aspect between them is security and how the cloud providers assure it. In healthcare systems, cloud not only facilitates the exchange of electronic medical records but it also enables to share the contents in a secured way. These types of medical records sharing systems will improve the storage contents security to be shared across all healthcare establishments include one hospital sector to other. With quick and secured access is very essential to share the medical records.

The proposed research work aims at securing the DICOM content storage in a Trustworthy Medical Cloud and access control based authentication for accessing the DICOM contents. A novel access control based on RSA OTP generation is proposed in this paper is to ensure the confidentiality of the stored DICOM content in public cloud. The DICOM contents are stored on cloud to improve the quality and security of the patient details in healthcare systems. The authentication mechanism for users to access the DICOM content in cloud is also provided which will enhance the security of Dicom content in a public cloud. The access control mechanism will ensure whether the content is accessed by authorized person or not. With the help of proposed method, DICOM contents can be stored in a secured manner. The proposed authentication based access control mechanism will improve the confidentiality and integrity of the patient details in health care management systems.

Future Work:

In future this system may be extended for implementation in commercial applications like Amazon aws and provide greater security services to the end users in the cloud environment.

Contributions:

This paper makes the following contributions;

- Proposed a randomized encryption methodology to ensure the privacy of DICOM medical contents.
- Stores the DICOM contents in a cloud by a secured manner.
- Proposed authentication mechanism is to ensure the stored DICOM contents privacy and confidentiality.

REFERENCES

Balamurugan, S. *et al*., 2015, "NGCC: Certain Investigations on Next Generation 2020 Cloud Computing-Issues, Challenges and Open Problems", Australian Journal of Basic and Applied Sciences, 9(33): 234-241.

Balamurugan, S. *et al*., 2015. "A Survey on Context-Aware Monitoring Strategies for Cloud Based Healthcare Systems", Australian Journal of Basic and Applied Sciences, 9(31): 31-35.

Chenghao He *et al*., 2010. "A cloud computing solution for Hospital Information System", http://ieeexplore.ieee.org/document/5658278.

Chia-Chi Teng *et al*., 2012. "Mobile Ultrasound with DICOM and Cloud Connectivity", Proceedings of the IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI 2012) Hong Kong and Shenzhen, China, pp: 667-670.

Cloud computing principles, systems and applications NICK Antonopoulos http://mgitech.wordpress.com.

Deepak, G. and S.S. Dr. Manjunath, 2015. "Decentralized Secure Data Storage and Retrieval in Mobile Cloud Environment for Multi- Tenancy Management", Australian Journal of Basic and Applied Sciences, 9(36): 355-359.

Dhivya, S. and M. Ragulkumar, 2016. "A Secure Data Sharing In Public Cloud Using Des, Rc4 And Diffie Hasbe Algorithm", Australian Journal of Basic and Applied Sciences, 10(10): 81-87.

DICOM security chapter 11, ACR-NEMA (National Electrical Manufacturers Association files, pp: 247-261.

Digital Imaging and Communications in Medicine (DICOM) 2003. Part 15: Security Profiles, Published by "National Electrical Manufacturers Association" USA.

Hemlathadhevi, A. and Dr. Rajeshwari Mukesh, 2015. "Identity Based Encryption for Secure Data Access in Cloud Computing using Machine Learning Algorithms", Australian Journal of Basic and Applied Sciences, 9(33): 72-77.

Parthasarathy, S. and C. Jothi Venkateswaran, 2015. "Scheduling Jobs Using Oppositional- GSO Algorithm in Cloud Computing Environment", Australian Journal of Basic and Applied Sciences, 9(33): 145-155.

Rabi Prasad Padhy *et al*., 2012. "Design and Implementation of a Cloud based Rural Healthcare Information System Model", UNIASCIT, 2(1): 149-157.

Srinivasan, S. and K. Raja, 2016. "Ensuring Cloud Security and Privacy Through Enhanced Merkle Hash Tree Method Using Bat Mechanism", Australian Journal of Basic and Applied Sciences, 10(1): 676-684.

Subhasri, P. and Dr.A. Padmapriya, 2013. "Multilevel Encryption for Ensuring Public Cloud", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), 3(6): 527-532.

Subhasri, P. and Dr. A. Padmapriya, 2015. "Enhancing the Security of Dicom Content Using Modified Vigenere Cipher", International Journal of Applied Engineering Research, ISSN 0973-4562, 10(55): 1951-1956.

Suhaila Mohammed *et al*., 2017. "Block-based Image Steganography for Text Hiding Using YUV Color Model and Secret Key Cryptography Methods", Australian Journal of Basic and Applied Sciences, 11(7): 37-41.

Suresh, M. and C. Kavitha, 2015. "Time Sensitive Data Stream to Achieve Intrusion Prevention in IaaS Cloud", Australian Journal of Basic and Applied Sciences, 9(33): 51-55.

The ultimate guide to implementing a medical image sharing portal, http://www.dicomgrid.com/, last accessed on 15/10/2016.

Wan Rozaini Sheik Osman, *et al*., 2017. "Factors That Influence The Adoption Of EHR By Health Professions: The Case Of Dhi-Qar Hospital", Australian Journal of Basic and Applied Sciences, 11(5): 169-175.