Cloud based Framework for Secure Sharing of Medical Reports

Jayashree Katti
Pimpri Chinchwad College of Engineering
Pune, India

Aparna M. Lanjekar
Pimpri Chinchwad College of Engineering
Pune, India

Apurva K. Thakur
Pimpri Chinchwad College of Engineering
Pune, India

Yaminee A. Koli
Pimpri Chinchwad College of Engineering
Pune, India

ABSTRACT
Cloud computing has recently emerged as a new paradigm for hosting and delivering services over the Internet which define the shape of a new era. Cloud computing is the changing way to store, compute and use the data and resources which are stored on the remote servers due its properties such as it provides robustness, on-demand self-service, measured resources, broad network access and low cost. But data leakage, insecure interface and sharing of resources are the major issue that prevents users from storing files on the cloud. Everyday extensive amount of data is generated in multi-specialist hospitals. This article presents various techniques to protect electronic medical reports (EMR)in various forms like images, videos or documents etc. stored on cloud. If doctors of various specializations want to view the reports it will be easy for them if those are placed on the cloud. This will also help patient in not carrying the prescriptions or big size reports. This article addresses these issues by proposing Advanced Encryption Standard (AES) for securing the multiple EMR. In order to prevent issues like breaches and malware attacks on cloud, this innovative scheme helps in high level security to safeguard the files or reports that are stored on the cloud.

Keywords
Cloud Computing, Advanced Encryption Standard (AES), Electronic Medical Reports (EMR).

1. INTRODUCTION
Medical records are central to all patient healthcare activities. The main reason for maintaining medical records is to ensure continuity of care for the patient. Healthcare organizations are expected to provide new and improved patient care capabilities. Information Technology plays an important role in the health and patient care arenas, with cloud computing beginning to make its mark. With the adoption of cloud computing approaches in the healthcare sector by most health institutions, medical image data are stored remotely in third party servers. To ensure confidentiality and authentication methods privacy, safety and security needs to be guaranteed for such digital data by engaging encryption to ensure authorship. Cloud is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer[3]. Cloud Computing allows us not only to access the applications as utilities, over the network but also to create, configure, and customize the business applications online. Cloud computing, the environment that offers resources encapsulation on the Internet in the form of dynamic, scalable, and virtualized services, presents a variety of on demand services to the public such as the telemedicine services[3]. In spite of the cloud computing advantages, it has a number of disadvantages such as the data security which considered a major problem that face the users of this technology since they outsource their data to distributed storage systems and not a local one. Therefore, when transferring user's data over the cloud environment, especially the medical data, this kind of data which contains crucial information about the patients, a high level of protection of the integrity and confidentiality of these data have to be guaranteed to overcome any attacking attempts that may face these transmitted data. The Advanced Encryption Standard, also known as Rijndael. The Advanced Encryption Standard is a specification for the encryption of electronic medical data. AES is based on a design principle known as a substitution–permutation network, a combination of both substitution and permutation, and is fast in both software and hardware. The Advanced Encryption Standard provides the demonstration of encryption and decryption of images and videos to the users. Due to the strong security and operation efficiency, the proposed secure cloud computing system should be extremely suitable for use in Health Information Exchange through cloud computing environment [6].

2. RELATED WORK

2.1 Definition of Cloud
Cloud is the practice of using a network of remote servers hosted on the Internet to store, manage and process data, rather than a local server or a personal computer. Cloud Computing provides us a means by which we can access the applications as utilities, over the internet. It allows us to create, configure, and customize the business applications online.

5 Essential Characteristics of Cloud
1. On Demand Self-Service: In this customer can self-provision compute storage without human interaction.
2. Broad Network Access: Applications are available on the network and accessed through standard mechanisms.
3. Resource Pooling: To serve multiple consumers using multi-tenant model, the provider's resources are pooled.
4. Rapid Elasticity: Capabilities can be elastically released and provided by cloud provider.
5. Measured Service: It must be measured by performance with pay-as- you-go pricing model.

The data exchange framework is designed as part of healthcare services which the whole platform is deployed on cloud-based environment. The platform uses Platform-as-a-Service (PaaS) concept so that systems belong to any registered healthcare institutes can call the services and integrate them as part of their implemented healthcare applications. The architecture is divided into three layers; Infrastructure-as-a-Service (IaaS) layer, Platform as-a-

Service (PaaS) layer, and Software-as-a-Service (SaaS) layer.

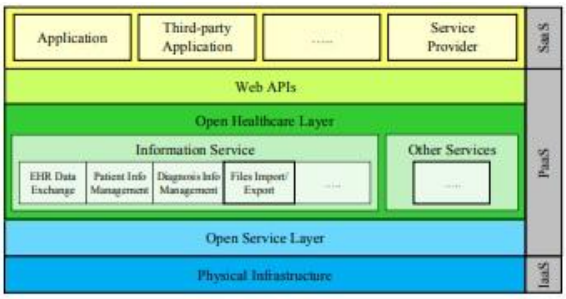

Fig. 1: Cloud architecture

1. IaaS layer: It manages resource and environment of physical machine to the virtual machine. Physical machine is in the physical infrastructure which consists of three main resources; server, storage, and network. This layer is all managed by the cloud provider

2. PaaS layer: It is deployed on cloud provider that can support requirement of the designed platform. It consists of two sub-layers; open service layer (lower layer), and open healthcare layer (upper layer)

a. Open service layer: It provides basic services such as processing unit, database management, and user management.

b. Open healthcare layer: It is the main layer of the platform for healthcare services. It provides following basic healthcare services: Patient information management, Diagnosis information management, Patient health service authority, Files import/export, Patient referral management, Pharmacy management, Prescription record and EHR data exchange. This layer can be developed based on open source software, such as Open MRS.

3. SaaS layer: The top layer of the architecture allows any third party software to run on the cloud platform. Services provided in the PaaS layer can be utilized by sending request messages through Web APIs. The EHR data exchange service is also included for convenient access. Many of the Open MRS services can also be made available. Healthcare institute can access third party software through web interfaces.

2.2 Video Encryption and decryption

With the fast growth of multimedia technology many hospitals across the world are using videos. Such sensitive data has to be protected either in transmission or storage. One possible way to protect multimedia information is to stop unauthorized access. But this approach cannot make sure that the multimedia information is physically secure. Another easy approach is to encrypt the complete bit stream with a cryptographic algorithm, such as DES or AES. However videos generally possess a large amount of data and require real-time operations. Different types of video applications require different levels of security.

3. PERFORMANCE PARAMETERS

To evaluate video encryption decryption algorithms there is a need to define a set of performance parameters.

1. Encryption Ratio: It is the ratio of size of encrypted video to the size of the original video. Lesser the ER better is the computational efficiency of the algorithm.

2. Compression Efficiency: The ease of compression depends on the data compression efficiency. Some encryption algorithms introduce additional information that is necessary for encryption/decryption. The size of the encrypted video should be as less as possible.

3. Degradation: This criterion measures the distortion of the video with respect to the original video. Visual degradation should be achieved to a considerable level so that the video is not understandable to the attacker. In highly confidential videos, high visual degradation is a must.

4. Security: The algorithm should be support to attacks such as brute-force and known-plaintext attack.

5. Format Compliance: Encrypted bit stream must be compliant with the compressor. The standard decoder should be able to decode the encrypted videos

6. Speed: For real-time applications the encryption and decryption time should be as less as possible.

4. PROPOSED METHOD

Health care has traditionally lagged behind other industries in implementing speedy, efficient communication of information. Medical data is a central part of diagnostics in today's healthcare information systems. Cloud helps to store, to manage and process voluminous data on remote servers. With the acceptance of cloud computing technology in the healthcare sector by most health institutions, medical image data are stored remotely in third party servers. Privacy, safety and security needs to be guaranteed for such digital data by engaging Advanced Encryption Standard algorithm to ensure confidentiality and authentication methods to ensure authorship. This system will consist of maintaining the privacy and security of patient health information exchange from organization threats and systemic threats.

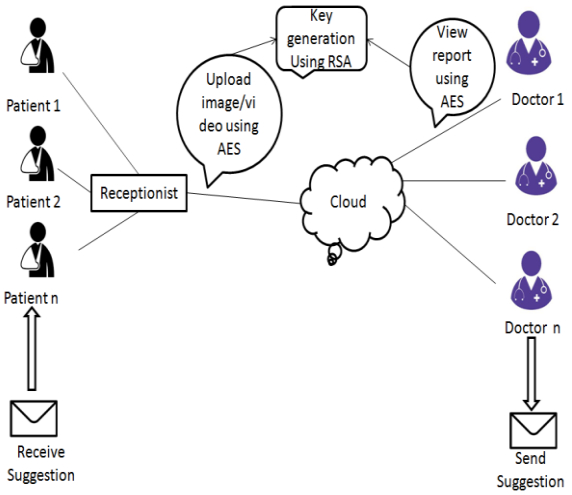

Fig. 2: Advanced Encryption Standard for Electronic Data Report Encryption and Decryption

In this system, electronic medical reports are secured by using AES-128 algorithm for transmission of EMR over cloud. The AES key is again encrypted and decrypted using RSA public key cryptography to securely share the AES key between receptionist and doctor. The AES key is encrypted

using public key of doctor and shared to doctor over the network. To get original key, doctor can use his private key to view the report of patient.

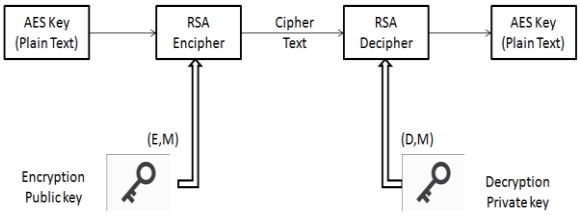

Fig. 3: Key Generation using RSA algorithm:

AES algorithm is of three types i.e. AES-128, AES-192 and AES-256. This classification is done on the bases of the key used in the algorithm for encryption and decryption process. The numbers represent the size of key in bits. This key size determines the security level as the size of key increases the level of security increases.

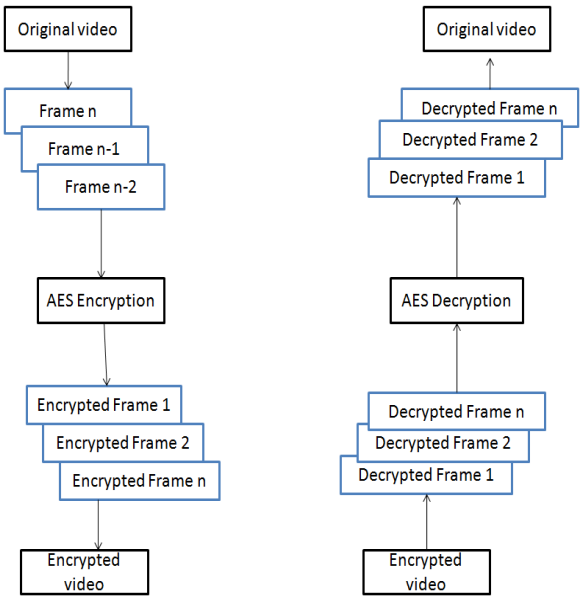

Fig. 4: Video Encryption and Decryption using AES

5. RESULT

The pixel value distribution of each image can be reflected by PSNR i.e. Pick Signal Noise Ratio. The term Pick Signal Noise Ratio is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation.

Original Image

PSNR value = 0.0dB

Encrypted Image

PSNR value = 24.84 dB

Decrypted Image

PSNR value = 0.031 dB

Fig. 5: PSNR values for Medical Report

For computing upload and download time from cloud the results videos of length 2 sec to 55 sec has been taken. We have taken number of video having length between 2 sec to 55 sec to calculate the time taken by video to upload and download from cloud. AES algorithm has been applied to encrypt and decrypt the original video having variable size in KBs.

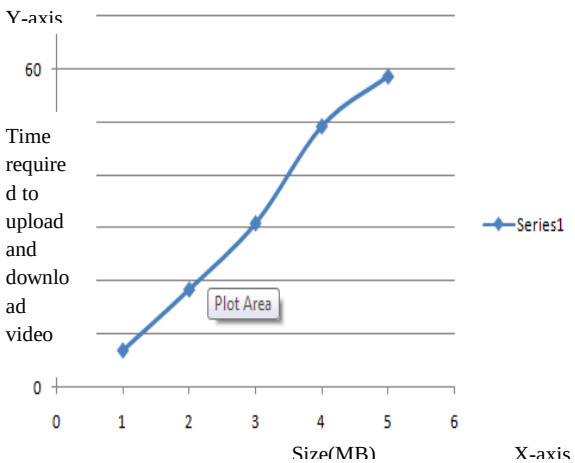

Fig. 6: Graph result length Vs time

Table. Video upload and download time from cloud

Video Size	Upload Time	Download Time
76.4 KB	0.05	0.07
101.8KB	0.07	0.10
2.3 MB	0.16	0.18
4.6 MB	0.27	0.28
5.1 MB	0.30	0.33

6. CONCLUSION

In this paper we used AES algorithm for video and image encryption. The Advanced Encryption Standard is a specification for the encryption of electronic medical reports. The proposed scheme improves the quality of patient care and also contributes to the management and moderation of health care costs. The AES algorithm is useful for encryption of EMR information to provide security while uploading on cloud. Using the proposed scheme, Doctors can appropriately access and securely share patients medical information electronically by improving the speed, quality, safety.

7. REFERENCES

[1] Cong Wang et al., "Ensuring data storage security in Cloud Computing", Quality of Service, 2009.

[2] Aeloor, Deepak, and Amrita A. Manjrekar. "Security Biometric Data with Visual Cryptography and Steganography."Security in Computing and Communications. Springer Berin Heidelberg,2013. 330-340.

[3] Ajay Kulkarni and Saurabh Kulkarni "Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study", International Journal of Computer Applications.2013

[4] S. Lian, Multimedia Content Encryption: Techniques and Application, CRC, 2008.

[5] Ako Muhammad Abdullah "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data",2017.

[6] Abdullah, A. M., & Aziz, R. H. H. (2016, June). New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm., International Journal of Computer Applications, Vol. 143, No.4 (pp. 11-17).,2017.

[7] Priya Deshmukh "An image encryption and decryption using AES algorithm", International Journal of Scientific & Engineering Research,2016.

[8] William Stallings, "Advance Encryption Standard," in Cryptography and Network Security, 4th Ed., India: PEARSON,pp. 134–165.

[9] Prof. A. B. Deshmukh "Video Frame Encryption Algorithm using AES", International Journal of Engineering Research & Technology (IJERT),2016.