*International Journals of Advanced Research in Computer Science and Software Engineering*
*ISSN: 2277-128X (Volume-7, Issue-8)*

**Research Article** | **August 2017**

# An Efficient Cloud Computing Security in Healthcare Management System

**M. Vignesh Mahalakshmi**
Research Scholar, P.G. and Research Department of Computer Science, Swami Vivekananda Arts and Science College, Orathur, Villupuram, Tamilnadu, India

**Dr. G. T. Shrivakshan**
Head, P.G. and Research Department of Computer Science, Swami Vivekananda Arts and Science College, Orathur, Villupuram, Tamilnadu, India

**DOI: 10.23956/ijarcsse/V7I8/0111**

***Abstract - Now-a-days Healthcare Sectors to create acloud computing environment to obtain a patient's complete medical record. This environment reduces time consuming efforts and other costly operations and uniformly integrates collection of medical data to deliver it to the healthcare specialists. Electronic HealthRecords have been usuallyimplemented to enable healthcare providers and patients to create, manage and access healthcare information from at any time and any place. Cloud environment provide the essential infrastructure at lower cost and improved quality. The Healthcare sector reduces the cost of storing, processing and updating with improved efficiency and quality by using Cloud computing. But today the security of data in cloud environment is not adequate. The electronic health record consists of images of the patient's record which is very confidential. The Electronic Health Records in the healthcare sector includes the scan images, X-rays,DNA reports etc., which are considered as the patients private data.It requires a very high degree of privacy and authentication. So, providing security for a large volume of data with high efficiency is required in cloud environment. This paper introduces a new mechanism in which the images of patient's record can be secured efficiently and the private data are well-maintained for later use. Since most of the private data are in the form of images, extra care must be taken to secure these images. This can be done by converting the images into pixels and then encrypting those pixels. After the encryption, the single encrypted file is divided into 'n' number of files and they are stored in the cloud database server. The original data is obtained by merging the n divided files from the cloud database server and then decrypting that merged file using the private key which is made visible only to the authorized persons as required by the hospital. To protect the data in cloud database server cryptography is one of the important methods. Cryptography provides several symmetric and asymmetric algorithms to secure the data. This paper presents the symmetric cryptographic algorithm named as Advanced Encryption Standard (AES).***

***Keywords: Cloud environment; Electronic Health Record; Security; Healthcare Data; Encryption; Decryption; Cryptography; Advanced Encryption Standard (AES).***

## I. INTRODUCTION

Cloud Computing is a technology which uses the internet and central remote servers to keep data and other applications. Cloud computing allows consumers and enterprises to use applications without installation and access their files at any computer through Internet access [2]. This technology provides efficient computing by centralized data storage, processing and bandwidth. Cloud computing has been proposed as the next-generation information technology architecture for enterprises.It is often provided a service over the Internet in the form of infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) [6]. Cloud computing is the broader concept of infrastructure convergence. This type of data centre environment allows enterprises to get their applications up and running faster, with easier manageability and less maintenance to meet business demands. The primary aspect of cloud computing is storing the data centralized [7]. From the user point of view, storing data remotely to the cloud in a flexible on-demand manner brings attractive benefits such as relief of the problem in case of universal data access with location independence, storage management and avoidance of capital expenditure on hardware,software components and personnel maintenance, etc., Hence cloud environment has abilities to provide service to users without reference to the infrastructure.

Even though the cloud computing has many advantages, there are number of disadvantages in it. The major disadvantage is providing security to cloud resources and data from unauthorized access. There are several security issues or concerns in cloud computing environment [13]. These problems are faced by both cloud providers and users. The problem could be either on network side or data side. Many security algorithms have been proposed for securing the cloud data where all the proposed security algorithms using the encryption technique. The AES and Pailier cryptosystem algorithm is used to encrypt the image and text files [1]. A Homomorphic Encryption Algorithm is also used to secure the data from unauthorized access [2]. Many encryption algorithms are being used to provide security to the data that are stored in cloud.

 

### *1.1 Cloud Architecture*

The architecture of Cloud Computing can be divided into two sections [12]. They are named as front-end and back-end. The front-end comprises the client's computer and the applications required to access and perform operations on the cloud computing system. All cloud computing systems are not necessary to have the same user interface as shown in figure 1.

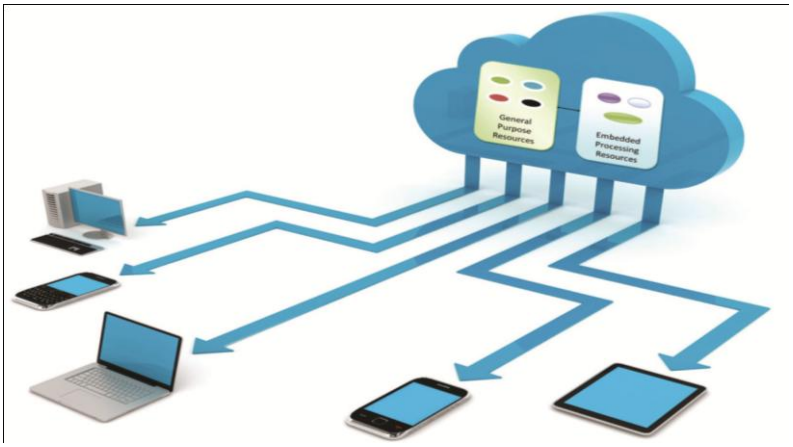


Figure 1: Cloud Basic Architecture

The back-end of the system hasvarious systems, servers and data storage systems which create the cloud of computing services.In theory, a cloud computing system can include any computer program, from data processing to video games. Each application has own dedicated server. A central server administers the system, monitors traffic and ensures that everything goes smoothly. It follows a set of rules which are called as protocols and uses a special kind of software called middleware. Middleware helps the networked computers to communicate with each other [10] . Mostly, servers don't run at full capacity,which means the processing power gets ruined. It is possible to fool a physical server to make it think that it's actually a multiple server, each running with its independent operating system. This technique is called as server virtualization. Server virtualization reduces the need for more physical machines by maximizing the output of individual servers.

### *1.2 Cloud Deployment Models*

*1.2.1Public Cloud*

In a public cloud, IT resources are made available to the public organizations and are owned by the Cloud service provider. The cloud services are made accessible to everyone via standard internet connection. In a public cloud, a service provider makes IT resources such as applications, storage capacities available to any consumer. This model is considered as an on-demand and pay-per use environment, where there are no on-site infrastructure or management requirements [5] . These benefits come with certain risks such as no control over the resources, data security, network performance and interoperability.

*1.2.2 Private Cloud*

In a private cloud, the cloud infrastructure operates separately for each organization and is not shared with any other organizations. This cloud model offers the greatest level of security and control. The two variations are as follows, o On-premise private cloud: This is also known as internal clouds and are hosted by an organization within their own data centers. This model provides a more standardized process, but is limited in terms of size and scalability [3].Thisis best suited for applications which require complete control of the infrastructure and security.Externally-hosted private cloud: This type of private cloud is hosted externally with a cloud provider, where the provider facilitates an exclusive cloud environment for a specific organization with full guarantee of privacy or confidentiality.

*1.2.3 Community Cloud*

A community cloud is a multi-tenant infrastructure that is shared among several organizations from a specific group with common computing concerns. Such concerns might be related to regulatory compliance, such as audit requirements, or may be related to performance requirements, such as hosting applications that require a quick response time.The goal of a community cloud is to have participating organizations realize the benefits of a public cloud but with the added level of privacy, security and policy compliance usually associated with a private cloud [11]. The community cloud can be either on-premises or off-premises, and can be governed by the participating organizations or by a third-party managed service provider.

*1.2.4 Hybrid Cloud*

In a hybrid cloud environment, the organization consumes resources from both private and public clouds.For the maintenance of service levels, the public cloud resources are imbibed with the private cloud resources. Organizations use their computing resources on a private cloud for normal usage, but access the public cloud for peak load/high requirements [10]. This ensures that a sudden increase in computing requirement is handled gracefully.

 

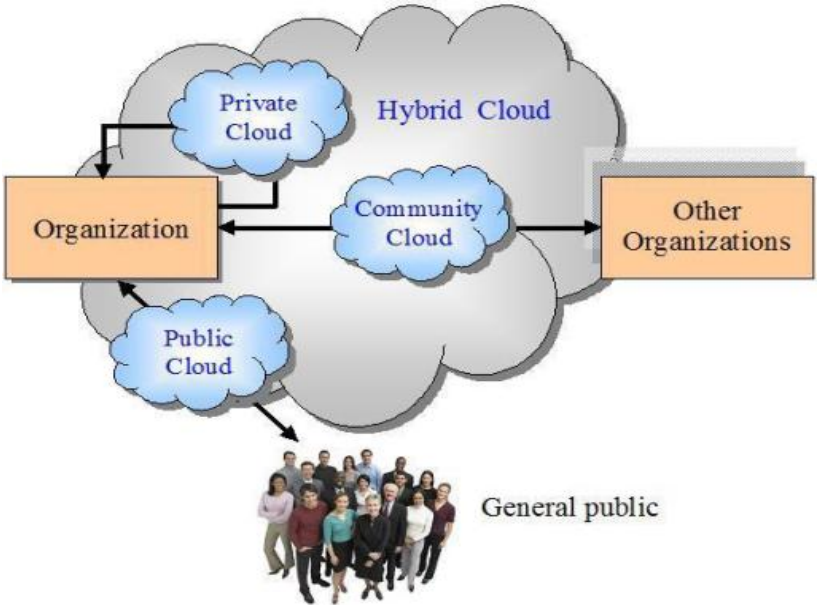


Figure 2: Cloud Deployment Model

***1.3 Cloud Service Models***

*1.3.1 Infrastructure as a Service (IaaS)*

IaaS provides virtual storage, virtual machine, virtual infrastructure, and other hardware components as resources that clients can provision [2]. The IaaS service provider manages all the infrastructure, while the client is responsible for all other aspects of the deployment. This can include the applications, operating system and user interactions with the system as shown in figure 3.

*1.3.2Platform as a Service (PaaS)*

PaaS provides virtual machines, operating systems, services, applications, transactions, development frameworks and control structures [7]. The client can deploy his/her application on the cloud infrastructure or use applications which are programmed using languages and tools that are supported by the PaaS service provider. The service provider controls the cloud infrastructure, the operating systems, and the enabled software. The client is responsible for managing and installing the application which it deploys.

*1.3.3 Software as a Service (SaaS)*

SaaS is the top most layer of the cloud computing stack, which is directly consumed by the end user. The consumer can make use of the service provider's application that runs on a cloud infrastructure. It is accessible from various client devices through a thin client interface such as web browser [9]. They offer many advantages such as reducing the need for infrastructure because they provide storage and compute powers remotely which also reduces the need for manual updates as it could perform those tasks automatically.

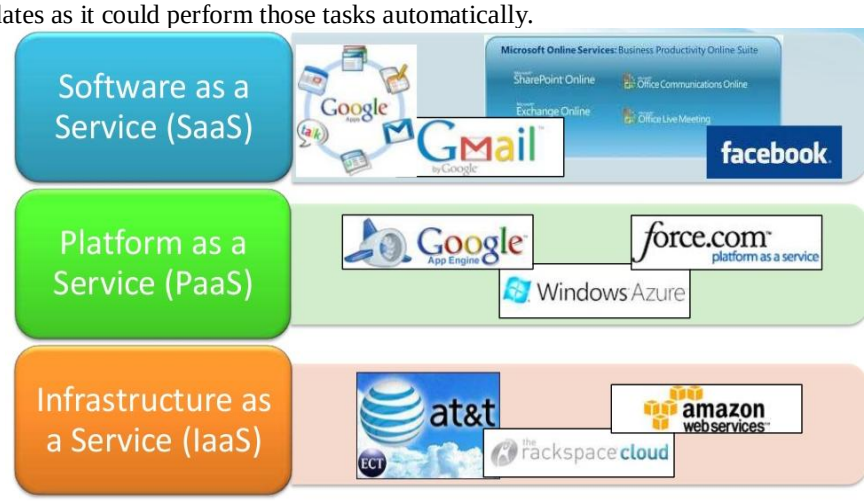


Figure 3: Cloud Service Model

## II. CLOUD FOR HEALTHCARE SECTORS

Now a days a healthcare environments need an infrastructure which reduces time consuming efforts and costly operations to obtain a patient's complete medical record and uniformly integrates collection of medical data to deliver it to the healthcare professionals. Electronic health records to enable healthcare providers, insurance companies and

patients to create, manage and access healthcare information at any situations. All the healthcare industries need to handle more requests with the available resources. The main objective of all the healthcare organization is to increase the number of people getting access to healthcare services [7]. To enhance the quality of service the healthcare industries demand more computation ability because of the amount of data that need to be stored, processed and updated is increasing exponentially. Cloud computing environment improves patient care by providing better,faster, secure and universal services at a lower cost and which meets the requirements of the healthcare sector. So the healthcare providers are more willing to move their systems to clouds that can remove the geographical distance barriers among health care providers and patients. With cloud computing, different doctors can access a patient's health records even if they're miles apart. These physicians need not have a direct communication to request for a transfer of health records [11]. They can just access them through clouds.

## III. LITERATURE REVIEW

**S. Aruna Devi et. al [1],** proposed a novel framework to recognize patient-centric privacy for personal health records in cloud computing. Patients themselves encrypt the data using encryption tools and their attributes are used for double encryption by CSP. The framework addresses the challenges brought by multiple PHR owners and users, by reducing the complexity of key management when the number of owners and users in the system is large. The advantage of this system is the data is automatically encrypted or decrypted right before it is loaded or saved. The disadvantage of this system is Complexity in key management.

**Nishitha Ramakrishnan et. al [2],** proposed a detail design of implementation of Hospital Management System for secure sharing of personal health records in Cloud Computing is performed. After considering the fact that cloud servers are partially trust worthy, in order to ensure security of Patient Health Record they encrypting the data before it can be stored it into the cloud environment. The proposed model uses different modules like admin, patient, hospital, doctor works in coordination and forms a complete and efficient Hospital Management System. The advantage of this system is to reduce the complexity of key management when number of owners and users in the system is large. The disadvantage of the proposed system is the private and public key is based on the large prime numbers.

**Divya Raval et. al [3],**proposed a system which system provides an environment where patient's records are stored and it will be referenced by the doctors to improve the efficiency of the treatment. This system handles the medical history of each individual of the country and provides access to all registered hospitals to read or update the data. The hospital which accesses the database must be registered and must have got a license. The license number is used as a unique code to access the database. The details of the patients will be stored and an identification number will be generated when their data are stored into the database for the first time after the implementation of the system. Whenever they go for a treatment, their medical data will be stored into the database using their identification number. For security reasons, any person who wants to view their data will be allowed only to read the data. The advantages of proposed system is to achieving data confidentiality and identity privacy with high efficiency, efficiently realizing access control of patient's personal health information,resist various kinds of malicious attacks and far out performs previous schemes in terms of storage, computational and communication overhead. The disadvantages of the system is the adoption of the cloud is progressing slowly.

**Jemal Hanen et. al [4]** ,defines a hybrid System that combines Multi-Agent System, Web Service and Mobile Cloud Computing. The proposed system only detail the MCC and healthcare web services. The main functionality of the prototype is to provide users with a mobile interface to manage healthcare information; the applications' platform is a tool for several users. The proposed MCMAS can achieve successful and proficient forecast for the majority of users. The proposed MCMAS has the benefits such as an ergonomic user interface through a mobile device and a mobile cloud services accessed anywhere anytime. The proposed MCMAS was designed and developed for just a polyclinic.

**Abha Sachdev et. al [5] ,** the proposed model used two different encryption techniques to protect the data from unauthorized access. They used Pailier cryptosystem to encrypt the images and to encrypt the text filesAES algorithm is used.

**Dr.S.Gunasekaran et. al [6] ,**proposed a homomorphic encryption technique to secure the data. They analyzed how cloud homomorphic encryption with splitting $^{key}$ and key delegation can help in securing the healthcare data. They proposed an FHE algorithm with key delegation to ensure data privacy in multilevel hierarchical order.

**Rashmiet. al [7],**proposed a secure cloud storage system supporting privacy-preserving public auditing.To provide security, third party auditors are used. The third-party auditors perform audits for multiple users simultaneously and efficiently.

**Santosh et. al [8],** the authors focused on data integration using Data Integrity protection scheme for preserving its intrinsic properties of fault tolerance.

**Namita N. Pathak et. al[9] ,** the authorsfocused on data access control to enhance data security. The authors used Ciphertext-policy Attribute based encryption to encrypt the data.

## IV. RISKS IN CLOUD COMPUTING

Cloud computing has many risks like data confidentiality, data security and overhead. The data stored in the cloud is highly confidential, such as business records, patient records, military records etc. In order to secure the sensitive data from unauthorized access anappropriate encryption standard must be applied to data stored in cloud. Most of the time data that is being stored or processed in cloud are in large numbers and the cloud servers sometimes become lazy

 

while computing that affects the correctness of the end result. Therefore the computation has to be made transparent [5]. Healthcare data mainly contains of large media files such as X-ray, CT scans,radiology and other type of images and videos, such files are called as the Electronic Health Records that are stored in distributed storage. The Electronic Health Records holds the healthcare sector people and the patients from all forms of misinterpretation like doctor's handwriting, losing prescriptions etc. The Electronic Healthcare Recordsis to enable healthcare providers and the patients to create, manage and access patient's healthcare information from anywhere and at any time. Thus, a patient's Electronic Health Records can be found distributed throughout the entire healthcare sector. Typically, an Electronic Health Record contains sensitive information such as person's health disorders and their pictures. These sensitive information are the most confidential ones and needs to be protected. To put everything in the cloud in an unencrypted is a big risk [12]. The data security in healthcare has been in exist for a long time, but since cloud computing gains more and more attention, healthcare providers are aiming at utilizing cloud's advantages to their benefit. However, these advantages come at a cost of various information security risks that need to be carefully considered. Risks vary depending on the sensitivity of the data to be stored or processed, and how the chosen cloud vendor has implemented their specific cloud services.

## IV. EXISTING SYSTEM

The existing system uses Pailier cryptosystem to convert the images into pixels. The array of pixels is then converted into matrix of pixels according to the dimension of the image. This matrix is encrypted using the homomorphic encryption method. The Advanced Encryption Standard (AES) technique is used for encrypting the text files. The decryption of the encrypted files is done after the retrieval from the cloud. The decryption is done using the private key which is present with the doctors and other physicians who use the Electronic Healthcare Records to get the information about the patients.

### *4.1 Drawbacks in the Existing System*

In the existing system, the data can be retrieved easily from the cloud if the decryption key is known by anyone. There are a number of techniques available to hack the decryption key. Some of the techniques areBrute Force attack, Key Search technique, Crypt Analysis and Systems-Based attack. The existing system provides single layer protection to the Electronic Healthcare Records.

## V. PROPOSED SYSTEM

The proposed system provides two-layer protection to secure the Electronic Health Records. In the first layer, the images and the text files are encrypted using Advanced Encryption Standard. In the second layer, the encrypted files are divided into n files. These n files are then stored in the cloud. The original Electronic Health Record can be decrypted only if the n files are merged. For splitting and merging the ciphertexts, a sequence key will be used. The overall architecture of the proposed system is shown in Figure 1.4.

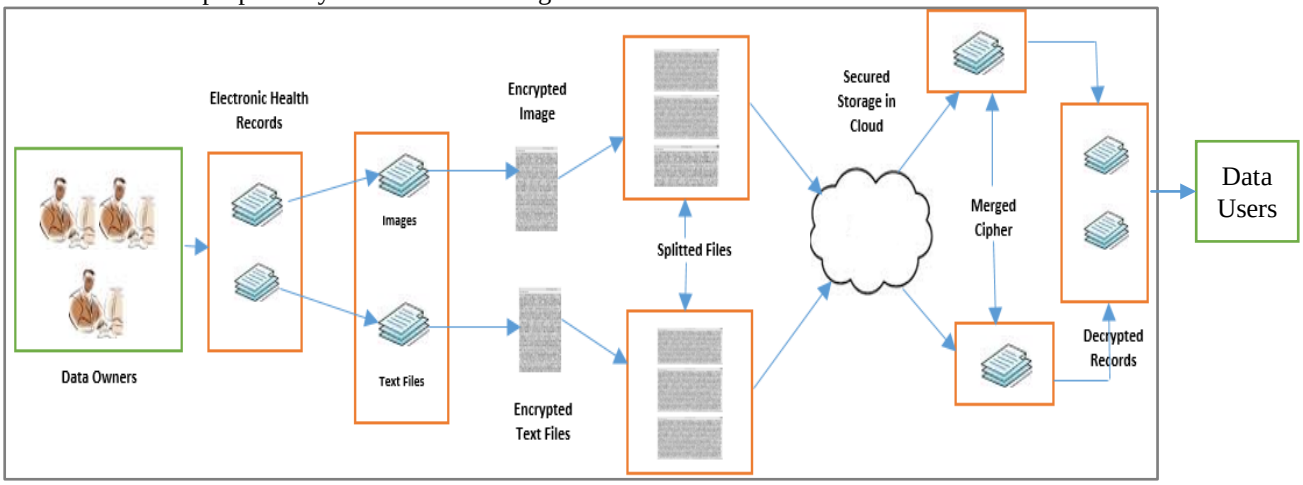


Figure 4: Architecture of the Proposed System

The proposed system includes the following six components

*(i) Data Owners*

The data owners are the patients whose informationis stored as Electronic Health Records. When a patient is in need of a treatment they need not spend time and effort in explaining his medical history because the hospital maintains Electronic Healthcare Records of the patients. As Electronic Health Records are stored in cloud the patients does not have to maintain paper health reports as well. They can also be shared with other healthcare institutions when required, with prior consent from the patients.

*(ii) Electronic Healthcare Records*

The patient information that are stored digitally is called as Electronic Health Records. The Electronic Health Records contains patient information like the patient's medical history, scan reports, X-rays, their current medications,

 

etc. that require high confidentiality. These Electronic Health Records can be stored in cloud, these records can be updated and processed whenever and wherever necessary. They also become readily accessible to the specified doctors and users. Since these Electronic Health Recordscan be in the form of text and multimedia data like the images, different methods have been implemented to secure the different formats of data in the Electronic Healthcare Records.

*(iii) Encryption*

The Advanced Encryption Standard (AES) encryption algorithm can be used to encrypt the Electronic Health Records. It is a symmetric encryption algorithm in which the same key is used to both encrypt and decrypt files. The key size used to encrypt the plain text is 128 bits. This algorithm helps in encrypting both the text and image files.

*(iv) Sequence Key*

To split and merge the ciphertexts the sequence key is used. After encryption, the ciphertext will be splitted into 'n' ciphertexts. Before decryption, to get the original ciphertext the splitted ciphertexts will be merged. Based on the sequence key the encrypted files are divided into 'n' files. The sequence key is entered by the physician or other authorized persons. There should be at least 8 characters in the sequence key. The value of 'n' depends on the length of the sequence key. For example, if the sequence number is entered as bfdk5467 (Length = 8), then the encrypted files will be divided into 8 files. The sequence key will be considered as valid only if it satisfies the following conditions

- The sequence key should not contain any space.
- The frequency of each character in the sequence key should be 1.
- The length of the sequence key must be at least 8.

Sample invalid sequence keys:

- bdfk 1547 – Space is used.
- bdfk2122 – The character '2' is used more than once.
- bdfk212 – Length is lesser than 8.

For splitting and merging the files the same sequence key is used. The first and the last character in the splitted file would be the characters in the sequence key. The first character specifies the index of the current file and the last character specifies the index of the next file that need to be merged with the current file.

*(v) Cloud Storage and Retrieval*

After the ciphertext is splitted, the splitted files are stored in the cloud data storage. Cloud data storage provides services as required by the clients in easy way. The cloud data storage offers the required resources to store the large volume of Electronic Health Records at low price. The services provided by the cloud are of good quality and appropriate for the healthcare sector. The physicians and doctors can easily retrieve the updated Electronic Healthcare Records from the cloud whenever it necessary. The storage and retrieval time is also less when cloud resources are utilized. The Electronic Health Records can beretrieved from the cloud and then decrypted after merging the ciphertexts.

*(vi) Decryption*

The splitted ciphertexts will be retrieved from the cloud and then merged to get the original ciphertext. After merging the splitted ciphertexts the decryption will be done. The decryption is done with the help of a private key which is made available to the doctors and other users who need the healthcare data. The key is generated from the Advanced Encryption Standard (AES) algorithm. The AES algorithm can be used for decrypting the text files.
Proposed Algorithm:

***1. Encryption and Splitting Algorithm***

*Step 1*: Read the Electronic Health image/text file
*Step 2*: Encrypt the image/text file using AES algorithm
*Step 3*: Generate Sequence Key
*Step 4*: Split the Encrypted image/text file into 'n' files using Sequence key
*Step 5*: Splitted encrypted file are stored into cloud data storage

***2. Merging and Decryption Algorithm***

*Step 1*: Read the encrypted file from the cloud data storage
*Step 2*: Merge the encrypted file using Sequence Key
*Step 3*: Decrypt the merged file using AES algorithm

## VI. RESULT AND DISCUSSION

The following snapshots show the original Electronic Health Record and its encrypted form, which is followed by the user defined sequence key and also the splitted ciphertexts, which is generated as a result of the predefined sequence key.

Figure 5: (a) Original Health Record (b) Encrypted Health Record

Figure 5 (a) and (b) depicts how data appear before and after encrypting the data. The left side image is the original Electronic Health Record (Plaintext) and the right side image is the encrypted Electronic Health Record (Ciphertext).


Figure 6: User defined Sequence Key to split the encrypted Electronic Health Record

Figure 6 depicts the input screen that asks for the user defined sequence key to split the encrypted Electronic Health Record. The same sequence key should be used while merging the splitted Electronic Health Records.

Figure 7: Splitted Electronic Health Records

Figure 7 shows a set of splitted files that are splitted using the above entered sequence key. The characters in the sequence key are used as the index of the splitted files, which will be removed in the merging process.

## VII. CONCLUSION

Cloud Computing is a set of IT Services that are provided to a customer over a network and these services are delivered by third party provider who owns the infrastructure.The central data storage is the key facility of the cloud computing it is of prominent importance to provide the security.The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography. Security goals of data cover three points

namely: Availability, Confidentiality, and Integrity.The proposed mechanism choose symmetric cryptosystem as solution as it has the speed and computational efficiency to handle encryption of large volumes of data. In symmetric cryptosystems, the longer the key length, the stronger the encryption. The AES algorithm is most frequently used encryption algorithm. This algorithm is based on several substitutions, permutations and linear transformations, each executed on data blocks of 16 byte whereas no possible attack against AES algorithm exists. Therefore, AES algorithm remains the preferred encryption standard for governments, banks and high security systems around the world. In this paper, a new mechanism is proposed to protect the healthcare data in the cloud using AES algorithm. The proposed system has a double layer protection in which the Electronic Health Records are stored in the cloud. In one layer the Encryption or Decryption will be done and in the other layer the Splitting or Merging of the ciphertext will be done. Thus, data security can be improved in cloud computing. As the proposed system is in the development stage, the actual results will be shared in future publication.

**REFERENCES**

[1] Aruna Devi. S and Manju.A, "*Enhancing Security Features in Cloud Computing for Healthcare using Cipher and Inter Cloud*", International Journal of Research in Engineering and Technology (IJRET), Volume 03 , Issue 03, Pages 200-203, Mar-2014.

[2] Nishitha Ramakrishnan and Sreerekha. B, "*Enhancing Security of Personal Health Records in Cloud Computing by Encryption*", International Journal of Science and Research (IJSR), ISSN 2319-7064, Volume 4 Issue 4, Pages 298-302 , April 2015.

[3] Divya Raval and Smita Jangale, "*Cloud based Information Security and Privacy in Healthcare*", International Journal of Computer Applications (IJCA), ISSN 0975 – 8887, Volume 150, Issue 4, Pages 11-15, September 2016.

[4] Jemal Hanen , Zied Kechaou and Mounir Ben Ayed, "*An enhanced healthcare system in mobile cloud computing environment*", Vietnam J Comput Sci , ISSN 267–277,Springer,Pages 267-277,2016.

[5] Abha Sachdev and Mohit Bhansali, "*Enhancing Cloud Computing Security using AES Algorithm*", International Journal of Computer Applications (IJCA) ISSN 0975 – 8887, Volume 67, Issue 9, April 2013.

[6] Dr.S.Gunasekaran and M.P.Lavanya, " *A Review On Enhancing Data Security In Cloud Computing Using Rsa And Aes Algorithms*", IJAER, ISSN 2231-5152,Volume 9, Issue 4 ,April 2015.

[7] S. Rashmi , Ghavghave, Deepali and M. Khatwar, "*Architecture for Data Security In Multicloud Using AES-256 Encryption Algorithm*" , International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), ISSN: 2321-8169,Volume 3, Issue 5, April 2017.

[8] Mr. Santosh, P. Jadhav and Prof. B. R. Nandwalkar, "*Efficient Cloud Computing with Secure Data Storage using AES*" ,International Journal of Advanced Research in Computer and Communication Engineering(IJARCC),ISSN 2278-1021,Volume 4, Issue 6, June 2015

[9] Namita N. Pathak and Prof. Meghana Nagori, *"Enhanced Security for Multi Cloud Storage using AES Algorithm*" ,International Journal of Computer Science and Information Technologies(IJCSIT), ISSN 0975-9646 , Volume 6, Issue 6, 2015.

[10] B. Vinoth Kumar, M. Ramaswami and P. Swathika, "*Data Security on Patient Monitoring for Future Healthcare Application*", International Journal of Computer Applications(IJCA), Volume 163 ,Issue 6, April 2017.

[11] B. Sri Varsha and, P.S. Suryateja, "*Using Advanced Encryption Standard for Secure and Scalable Sharing of Personal Health Records in Cloud*", International Journal of Computer Science and Information Technologies(IJCSIT),ISSN 0975-9646, Volume 5, Issue 6 , 2014.

[12] Prof. Pranali Kosamkar, Prachi Kadam, Shahista Shaikh, Rashmi Linganwar and Komal Mathpati, "*Different Levels of Security in Cloud*", International Journal for Scientific Research & Development(IJSRD),ISSN (online): 2321-0613, Volume 4, Issue 01, 2016.

[13] Rizwana Kowsar M.S, 2 Somasekhar T, 3DivyaShree K.B, 4 Pooja Giriraj, "*Design and Implementation of Security for Healthcare Billing System using Cloud Computing*", International Journal of Electrical, Electronics and Computer Systems (IJEECS), ISSN (Online): 2347-2820 , Volume -4, Issue-7,2016.

 