iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5156

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

Enhancing Security of Patient Health Records in Cloud Computing

Madhushree S. K[1], Sowmya. P[2], Manjunath C. R[3]
[1, 2, 3]*Jain University*

Abstract: ***Proficient Management of Hospital information and right upkeep of Patient Health Record (PHR's) is a critical test. The most imperative thing to be considered is the security of information which should be possible effectively by putting away PHR's utilizing Cloud Computing. Despite the fact that cloud information stockpiling gives a vital part of nature of administration as far as security, PHR's are scrambled utilizing AES Algorithm before it is been put away to the cloud condition. Electronic Health Records have been typically executed to empower medicinal services suppliers and patients to make, oversee and get to social insurance data from whenever and wherever. Cloud condition give the basic foundation at bring down cost and enhanced quality. The Healthcare area decreases the cost of putting away, handling and refreshing with enhanced effectiveness and quality by utilizing Cloud figuring. Be that as it may, today the security of information in cloud condition isn't satisfactory. The Electronic Health Records in the human services part incorporates the output pictures, X-beams, DNA reports which is exceptionally classified and are considered as the patient's private information. In this way, giving security to a substantial volume of information with high effectiveness is required in cloud condition. Another system is utilized as a part of which the pictures of patient's record can be secured effectively and the private information are all around kept up for later utilize. Since the greater part of the private information are as pictures, additional care must be taken to secure these pictures. This should be possible by changing over the pictures into pixels and after that encoding those pixels. After the encryption, the single scrambled document is isolated into 'n' number of records and they are put away in the cloud database server. The first information is gotten by consolidating the n isolated records from the cloud database server and after that decoding that blended document utilizing the private key which is made noticeable just to the approved people as required by the doctor's facility. To secure the information in cloud database server cryptography is one of the critical strategies. Cryptography gives a few symmetric and topsy-turvy calculations. To secure the information symmetric cryptographic calculation is utilized named as Advanced Encryption Standard (AES).***

I. INTRODUCTION

Cloud Computing has been proposed for enterprises as the next-generation information technology architecture. It is regularly given an administration over the Internet as framework as an administration (IaaS), stage as an administration (PaaS). Distributed computing is the more extensive idea of framework meeting.

This kind of server farm condition enables to get applications up and high speed running with less demanding sensibility and less upkeep to meet more business requests. Putting away information brought together is the essential part of distributed computing is. From the client perspective, securing data remotely to the cloud in a versatile on demand way brings charming favorable circumstances, for instance, help of the issue if there ought to emerge an event of boundless data access with region opportunity, amassing organization and avoidance of capital use on hardware, programming parts and work compel upkeep, et cetera., Hence cloud condition has abilities to offer organization to customers without reference to the structure.

Despite the fact that the distributed computing has numerous points of interest, there are number of limitations in it. The significant limitation is giving security in cloud assets and information from unapproved get to. In distributed computing condition there are a few security issues or concerns. These issues are looked from both cloud suppliers and clients. The issue could be either on arrange or information side. Numerous security calculations for securing the cloud information have been proposed where all the proposed security calculations utilizing the encryption procedure

To scramble picture and content documents.

The AES and Pailier cryptosystem calculation is utilized. To secure the information from unapproved get to a Homomorphic Encryption Algorithm is likewise utilized. Numerous encryption calculations are being utilized to give security for the information that are put away in cloud.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

A. Cloud Service Models

1) Infrastructure as a Service (IaaS). IaaS gives virtual capacity, virtual machine, virtual foundation, and other equipment parts as assets that customers can arrangement. The IaaS specialist organization deals with all the foundation, while the customer is in charge of every other part of the sending.

2) Platform as a Service (PaaS). PaaS gives virtual machines, working frameworks, administrations, applications, exchanges, improvement systems and control structures. The customer can convey their application on the cloud framework or utilize applications which are customized utilizing dialects and apparatuses that are upheld by the PaaS specialist organization. The specialist organization controls the cloud foundation, the working frameworks, and the empowered programming. The customer is in charge of overseeing and introducing the application that it sends.

3) Software as a Service (SaaS). SaaS is the first layer of the distributed computing stack, which is straightforwardly devoured by the end client. The purchaser can make utilization of the administration providers application that keeps running on a cloud framework. They offer numerous points of interest, for example, lessening the requirement for framework since they give stockpiling and register controls remotely which likewise decreases the requirement for manual updates as it could play out those undertakings consequently.

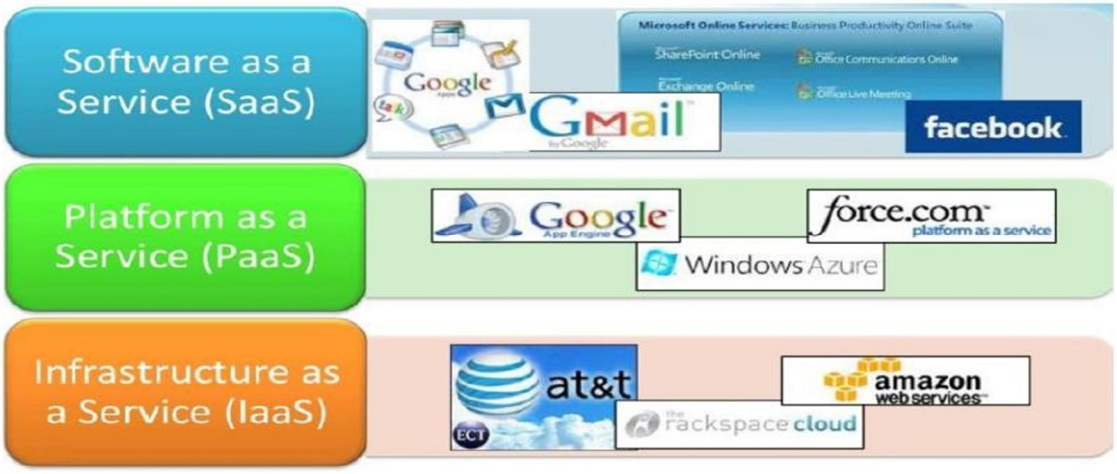


Fig. 1.1 Cloud Service Model

B. Problem Statement

Cloud computing for the Healthcare sectors lowers the storing cost, handling and refreshing with enhanced effectiveness and quality by utilizing Cloud registering yet the security of information in cloud condition isn't satisfactory. The electronic wellbeing record comprises of pictures of the patient's record which is exceptionally secret and are considered as the patient private information. It requires a high level of protection and confirmation. The most vital thing to be considered is the security of information which should be possible effectively by putting away Patient Health Records (PHR's) utilizing Cloud Computing.

C. Objectives

To give greater security to an extensive volume of information with high proficiency and high level of protection and validation by utilizing double layer insurance in AES algorithm.

II. LITERATURE REVIEW

S. Aruna Devi presented a novel structure to see understanding driven security for singular prosperity records are in appropriated figuring. Patients can themselves scramble the data using encryption gadgets and their characteristics are used for twofold encryption by CSP. The structure watches out for the challenges brought by different PHR proprietors and customers, by diminishing the diserse nature of key organization when the amount of proprietors and customers in the system is immense. The advantage of this structure is the data is subsequently mixed or unscrambled just before it is stacked or saved. The weight of this system is complication in key organization

Nishitha Ramakrishnan presented a detail blueprint of use of Hospital Management System for secure sharing of individual prosperity records in Cloud Computing is performed. In the wake of considering the way that cloud servers are to some degree trust exemplary, with a particular ultimate objective to ensure security of Patient Health Record they encoding the data previously it can

©IJRASET: All Rights are Reserved

be secured it into the cloud condition. The proposed demonstrate uses particular modules like executive, understanding, recuperating office, master works in coordination and structures a whole and capable Hospital Management System. The upside of this system is to diminish the multifaceted nature of key organization when number of proprietors and customers in the structure is considerable. The disadvantage of the proposed structure is the private and open key relies upon the broad prime numbers.

Sanjay P. Ahuja portray different utilizations of distributed computing over Healthcare, its suggestions. Patients and wellbeing associations take points of interest of the new innovation by enhancing patients nature of administration through a conveyed high-incorporated stage (Wang, 2010), organizing of restorative process and also diminishing IT foundation speculation or support costs which prompts a superior medicinal services condition. Focusing on the Global Market for Cloud Computing in Healthcare, IT ventures contribute vigorously to fabricate foundation for cloud to help it and enable associations to take profit by it. The rate of increment in receiving cloud is specifically relative to the rate of accomplishing more noteworthy efficiencies. This outcomes in providing uncommon sharing abilities between the social protection associations and patients alike.

The Challenges of Cloud Computing in Health Care is for the most part because of two essential concerns related with security and interoperability.

By exploiting arrangements accessible, the previously mentioned issues can be overcome. This prompts development towards cloud and exploiting the arrangements it give. Since Human services information is profoundly classified, its protection and security concerns should be handled. Security concerns can be tended to by following Health Insurance Portability and Accountability Act (HIPAA) while moving wellbeing record to the cloud. The human services information involves touchy data yet relocation of the restorative records to the cloud (outsider) might be trusted. To forestall revealing of data to unapproved people, security exercises, for example, forcing access controls, giving validation, checking approval should be possible. These issues are an obstruction that have moderated the cloud usage and ought to be tended to so as to empower the dependability of cloud frameworks.

III. EXISTING SYSTEM

The current framework utilizes Pailier cryptosystem to change over pictures into pixels. The variety of pixels is then changed over into framework of pixels as indicated by the measurement of the picture. This network is scrambled utilizing the homomorphic encryption technique. Advanced Encryption Standard (AES) method is utilized for scrambling the content documents. The decoding of the encoded records is done after the recovery from the cloud. The unscrambling is finished utilizing the private key which is available with the specialists and different doctors who utilize the Electronic Healthcare Records to get the data about the patients.

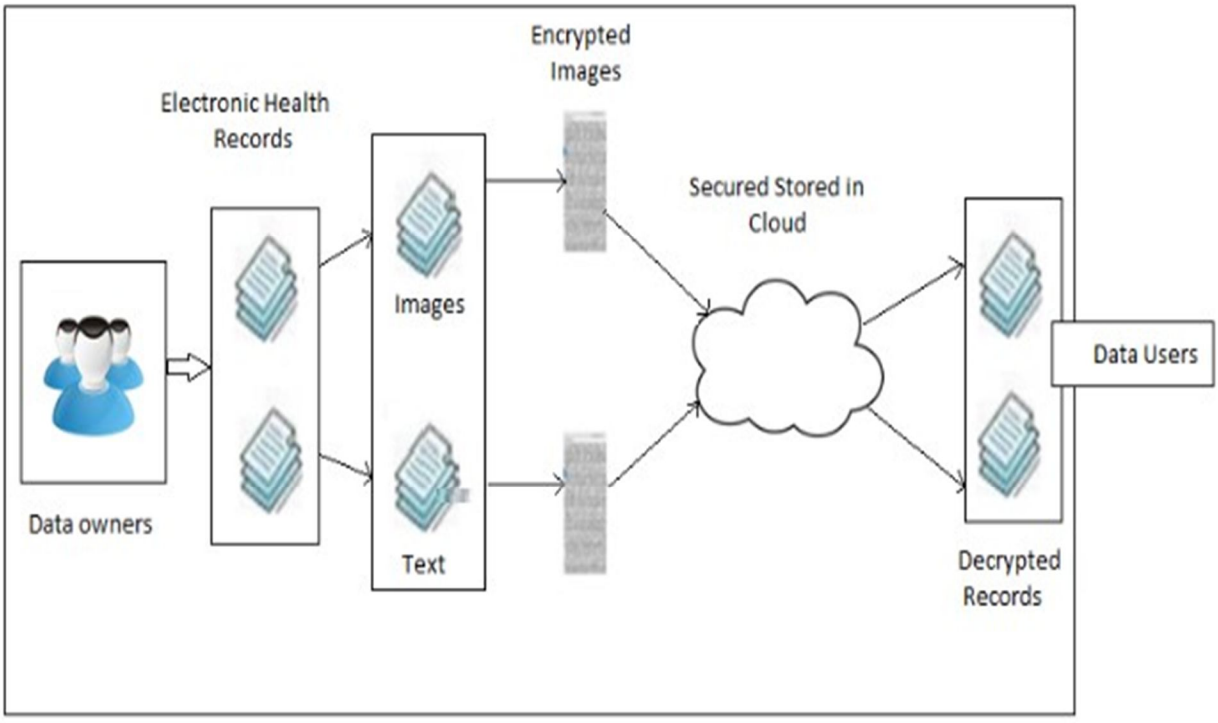


Fig.3.1 Existing System Architecture.

©IJRASET: All Rights are Reserved

A. Existing System Limitations

1) In the current framework, the information can be recovered effectively from the cloud if the decoding key is known by anybody.

2) There are various procedures accessible to hack the unscrambling key. A portion of the methods are Brute Force assault, Key Search strategy, Crypt Analysis and Systems Based assault.

3) The existing framework gives single layer protection for the Electronic Healthcare Records.

IV. PROPOSED SYSTEM

The proposed framework gives two-layer protection to secure the Electronic Health Records. In the primary layer, the pictures and the content documents are encrypted utilizing Advanced Encryption Standard. In the second layer, the encrypted documents are partitioned into n records. These n documents are then put away in the cloud. The first Electronic Health Record can be decoded just if the n documents are blended. For part and consolidating the cipher texts a succession key will be utilized.

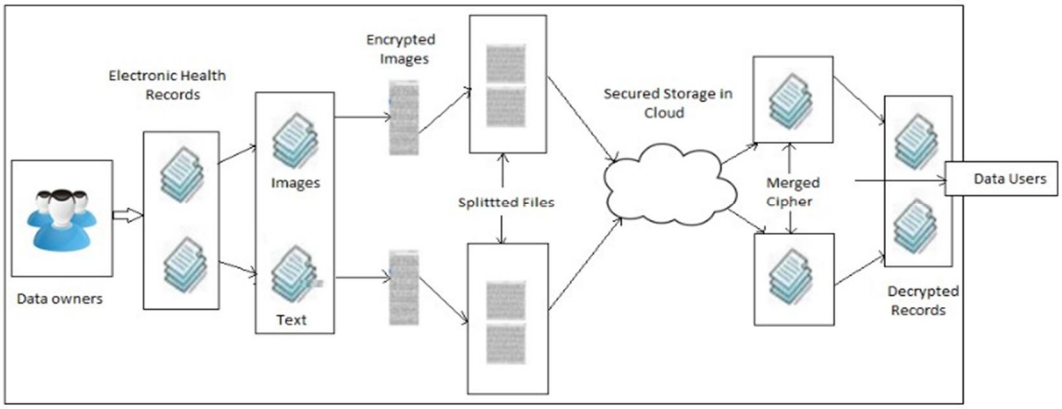


Fig.4.1 Proposed System Architecture.

Proposed framework incorporates the accompanying six parts

1) *Data Owners:* The information proprietors are the patients whose data is put away as Electronic Health Records. At the point when a patient need a treatment they require not invest energy and exertion in clarifying his medicinal history in light of the fact that the clinic keeps up Electronic Healthcare Records of the patients. As Electronic Health Records are put away in cloud the patients does not need to keep up paper wellbeing reports too. They can likewise be imparted to other medicinal services foundations when required, with earlier assent from the patients.

2) *Electronic Health Records:* The patient data that are put away carefully is called as Electronic Health Records. The Electronic Health Records contains quiet data like the patient's medicinal history, check reports, X-beams, their present prescriptions, and so forth that require high privacy. These Electronic Health Records can be put away in cloud, these records can be refreshed and handled at whatever point and wherever fundamental. They likewise turn out to be promptly available to the predefined specialists and clients. Since these Electronic Health Records can be as content and sight and sound information like the pictures, diverse techniques have been actualized to secure the distinctive configurations of information in the Electronic *Healthcare Records.*

3) *Encryption:* The Advanced Encryption Standard (AES) encryption calculation can be utilized to scramble the Electronic Health Records. It is a symmetric encryption calculation in which a similar key is utilized to both scramble and unscramble records. The key size used to scramble the plain content is 128 bits. This calculation helps in encoding both the content and picture records.

4) *Sequence Key:* To part and solidification the ciphertexts the gathering key is used. After encryption, the ciphertext will be splitted into "n" ciphertexts. Before unscrambling, to get the principal ciphertext the splitted ciphertexts will be mixed. In perspective of the course of action key the mixed reports are apportioned into "n" records. The course of action key is entered by the specialist or other endorsed individuals. There should be no under 8 characters in the course of action key. The estimation of "n" depends upon the length of the arrangement key. For example, if the progression number is entered as bfdk5467 (Length = 8), by then the encoded records will be parceled into 8 archives.

The arrangement key will be considered as legitimate just on the off chance that it fulfills the accompanying conditions

©IJRASET: All Rights are Reserved

a) The plan key should not contain any space.
b) The repeat of each character in the game plan key should be 1.
c) The length of the game plan key must be no under 8.

For part and uniting the records a comparable plan key is used. The first and the last character in the splitted record would be the characters in the gathering key. The essential character shows the rundown of the present record and the last character decides the rundown of the accompanying report that ought to be focalized with the present record.

5) *Cloud Storage Retrival:* After the ciphertext is splitted, the splitted documents are put away in the cloud information stockpiling. Cloud information stockpiling gives benefits as required by the customers in simple way. The cloud information stockpiling offers the expected assets to store the expansive volume of Electronic Health Records at low cost. The administrations gave by the cloud are of good quality and fitting for the human services part. The doctors and specialists can without much of a stretch recover the refreshed Electronic Healthcare Records from the cloud at whatever point it fundamental. The capacity and recovery time is likewise less when cloud assets are used. The Electronic Health Records can be recovered from the cloud and after that decoded subsequent to combining the ciphertexts.

6) *Decryption:* The splitted ciphertexts will be recovered from the cloud and after that converged to get the first ciphertext. In the wake of consolidating the splitted ciphertexts the decoding will be finished. The decoding is finished with the assistance of a private key which is made accessible to the specialists and different clients who require the social insurance information. The key is created from the Advanced Encryption Standard (AES) calculation. The AES calculation can be utilized for decoding the content document.

A. Proposed Algorithm

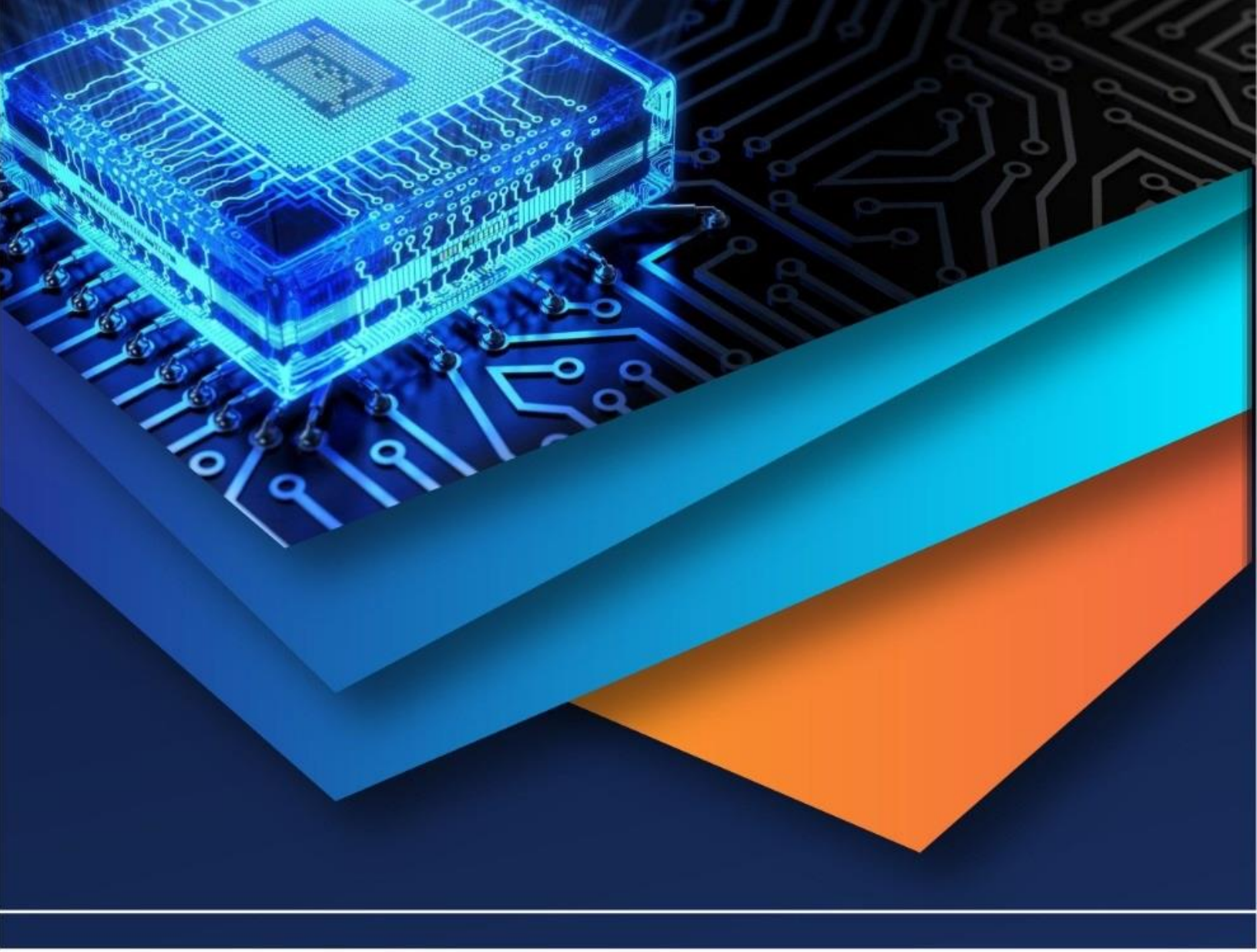
The proposed framework has double layer protection in which the Electronic Health Records are encoded utilizing Advanced Encryption Standard (AES) method in the principal layer and in the second layer the scrambled documents are separated into n documents. Hence, information security can be enhanced in distributed computing.

1) Encryption and Splitting Algorithm
a) Step 1: Electronic Health picture/content document are read
b) Step 2: Encrypting the picture/content document utilizing AES calculation
c) Step 3: Sequence Key is generated
d) Step 4: Encrypted picture/content document are encrypted into "n" records utilizing Sequence key
e) Step 5: Splitted encoded record are put away into cloud information stockpiling
2) Merging and Decryption Algorithm
a) Step 1: encoded record from the cloud information are read
b) Step 2: Merge the encoded record utilizing Sequence Key
c) Step 3: Decrypt the consolidated record utilizing AES calculation

V. CONCLUSION

Cloud Computing is an arrangement of IT Services that are given to a client over a system and these administrations are conveyed by outsider supplier who claims the foundation. The focal information stockpiling is the key office of the distributed computing it is of unmistakable significance to give the security. The craftsmanship and art of disguising the messages to present mystery in data security is perceived as cryptography. Security objectives of information cover three focuses to be specific: Availability, Confidentiality, and Integrity. The proposed system pick symmetric cryptosystem as arrangement as it has the speed and computational productivity to deal with encryption of huge volumes of information. In symmetric cryptosystems, the more drawn out the key length, the more grounded the encryption. The AES calculation is most every now and again utilized encryption calculation. This calculation depends on a few substitutions, changes and direct changes, each executed on information pieces of 16 byte though no conceivable assault against AES calculation exists. In this manner, AES calculation remains the favored encryption standard for governments, banks and high security frameworks around the globe. In this paper, another component is proposed to ensure the medicinal services information in the cloud utilizing AES calculation. The proposed framework has a twofold layer assurance in which the Electronic Health Records are put away in the cloud. Encryption or Decryption will be done in one layer the and Splitting or Merging of the ciphertext is done in other layer.. Accordingly, information security can be enhanced in distributed computing..

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)