Enhancing security of health record over cloud by using encryption algorithm

[1]Habtamu Shiferaw Adugna, [2]Mr.Raviraj Chauhan
[1]M.Tech Student (CSE), [2]Asst. Professor
[1] Department of Computer Science and Engineering,
[1]Parul University, Vadodara, India

Abstract: Cloud-based Health care services are newly growing up services technology. With the technological advancement, the lifespan of people has been changing in a day to today life. Cloud-based Health care provides remote care service for the rural and urban community and it needs high security and privacy. Cloud Computing has been widely used since it brings a great improvement in Healthcare. The Cloud Computing newly arising paradigm offers service for healthcare systems. Forwarding of sensitive medical data to the cloud environment involves different risk in case of the security and privacy. Both healthcare providers and cloud service providers must be concerning security and privacy of patient record information before moving to the cloud. The aim of this paper is identifying encryption algorithm used by cloud computing for enhancing security in health care sector and applying hybrid of three algorithms, RSA, AES and SHA-1.

Index Terms - **Telehealth, Cloud computing, Security, Privacy Encryption Algorithm**

I. Introduction

Health care sector is one of biggest organization in the world which helps the world's people in providing information about health for patients, doctors, medical students, and medical researcher and for health institution. The health care industry use Information Technology to address the accurate information for the listed above through the Internet. Using cloud computing technology to create link between the doctors, patient and health care institution through application software, services and store the record of those health care institution and patient in the cloud. Health care use electronic records and telecommunication technologies to help long distance clinical health care system, patient, doctor-nurse and related worker, professional health related education like medical person and public health administration. Health use different technology to address service to all those are internet, video conference, store and forward records, stream media and wireless communication. Health scope wide-ranging it covers the remote health care services, non-clinical services such as giving training, medical education.

Health care organization incorporates cloud computing paradigm in order to address the demand of health on data storage and cloud provider (CP) organization provide data storage server for health organization. Implementing cloud computing in health care is improving the work of physician, doctor, and nursing, patient in case sharing information but, the problem is the security and privacy of record at time of sharing and uploading into cloud server. However the flow of data over untrusted media due to that sensitive data can accessed by hacker or unauthorized person.

According to the definition of National Institution of Standard and Technology (NIST) cloud computing [9] is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The benefit of cloud computing in health care is patient's quality of service, sharing information across healthcare organizations, data can be accessed anywhere and everywhere by authorized entities, reduced capital expenditure, reduced operation risks, reduced complexity and maintenance, increased scalability flexibility and fast accessing of medical records of patient in remote area.

1.1. Cloud computing service Model

Cloud computing offer different service model those are Infrastructure as a Services (IaaS), Security as a service, Software as a Service (SaaS), and Platform as a Services (PaaS).

1. Software as a service (SaaS): It is a service model in which a user has to uses applications, but does not control hardware, network infrastructure and operating system on which application is done.
2. Platform as a service (PaaS): It is a service model in which a user does not manage cloud infrastructures like network, servers, operating system and storage, but has a power to control deployed and hosting application.
3. Infrastructure as a service (IaaS): A service model user has the ability to rent computing infrastructures like a computer, storage, network and other IT infrastructure.

1.2. Deployment models of cloud computing

Cloud computing deployment model those are Public cloud, Private cloud, community cloud and Hybrid cloud model.

1. Public cloud: It is available to general public. It is economical cloud that is stand-alone, proprietary based and off-premises. In house and small businesses use public cloud mostly to meet their requirements.
2. Private cloud: A cloud infrastructure is operated specially for a single organization.

3. Community cloud: The cloud infrastructure is shared by several organizations with common concerns (eg, mission, security requirements, policy, and compliance considerations).
4. Hybrid cloud: The cloud infrastructure comprises two or more clouds (private, public, or community).

II. Problems In Health Record Over Cloud Computing

In health care sector records need more security and privacy. However, moving those record to cloud has many risks because of insecure API, insecure data deletion and modification by hacker, session, malicious and worms, Trojan and lack of monitoring own data. But it possible to enhance the security of cloud record of health care service. Also cloud migration and threats can pose potential security and privacy risks for the health care information record. Privacy issue related to medical record in cloud are when owner of record has insufficient control over record on public cloud mainly when data is accessed and processed in cloud computing environment, sensitive information exposé to unauthorized person, record move to cloud, unauthorized secondary storage in cloud. However, these sensitive records of medical data should be accessed, retrieved and backup, data flow and dynamic provision of cloud in nature.

The biggest issue of moving Health care record into the cloud environment is the security problem of newly emerging cloud computing attacks and threat and the second problem is privacy issue of Cloud Computing is an Internet-based technology that shares processed records and resources along other connected device. They allow user and organization to store and process their record in the third parity data center (cloud provider server). Due to this application available in cloud technology most of customer, business man and different organization like health sector, education sector attract by cloud computing technology now a day. It play important role in the health care such as transforming paper based medical record into digital data, storing large data set, sharing information among hospitals and physician and store and retrieve data from remote area. To perform all the above activity of healthcare sector over cloud computing environment requires different security and privacy tools.

III. Literature Review

Many researchers have done their work on enhancing security of health record on cloud computing using different encryption algorithm. These researches are based on different techniques which have their own advantages as well as limitations.

According to [1] giving high degree of patient privacy by proving a security by classifying the data on the base of their sensitivity level and using encryption algorithm such as AES,RSA and Play-fair for confidentiality and integrity of data. Highly sensitive information of Electronic Health Record (EHR) is encrypting using Attribute Base Encryption (ABE)

According to [2] used two-layer for protection to the Electronic Health Record (EHR). In the first is layer using AES for encrypting of image and text and in the second layer encrypting cipher text is splitting into many parts and final merging ciphertext.

Author [3] presents the idea of joining Cipher Cloud, Inter Cloud and ABE schemes, offers an advanced method to enhance security features in the cloud by double encryption using algorithms and tools

According to the [4] zhifeng Xioa and yangioa Xioa the main challenges of building a secure and trust cloud technology is outsourcing of record, multi-tenant and massive data and intensive computation. Conduct his review based on attribute-driven Methodology and other supporting techniques. Based on this methodology and supporting techniques employs five attribute of security and privacy (confidentiality, integrity, availability, Privacy-preservability and transparency)

IV. Encryption Algorithm Used for Enhancing Security in Cloud

The different Algorithm that we will use to enhance the security and privacy of health care in cloud computing those are security protection mechanism and piracy-preserving. They protect record in cloud computing we use symmetric and asymmetric encryption algorithm [7] [8] [10]. Those algorithms are:

- Symmetric encryption
- Asymmetric encryption
- Hybrid encryption

Symmetric Encryption: It is convention key / private key/ single encryption. Both sender sand revisers shares same key. Examples of this encryption algorithm are [7]:

- DES (data Encryption Standard)
- 3DES (data Encryption Standard)
- AES (Advanced Encryption Standard) and
- RC4

Advantages of Symmetric Encryption: It is faster, encrypted data transferred on link and uses password authentication to prove the receivers identity Disadvantages of Symmetric Encryption: They have problem of key transportation and cannot give digital signature.

AES (Advanced Encryption Standard): It is a symmetric cryptographic encryption or a block cipher encryption algorithm and use the same key for both encrypt and decrypt block of cipher. It is vulnerable to brute-force and side channel attacks. More secure than DES, improved efficiency, supported block cipher is 128,192 and 256 bit.

DES (data Encryption Standard): It is a symmetric cryptographic encryption or a block cipher encryption algorithm and use the same key for both encrypt and decrypt block of cipher [7]. It is vulnerable to automated brute-force and linear and differential attacks. It is less efficiency than 3DES (data Encryption Standard) and 3DES (Data Encryption Standard improvement DES algorithm and overcome brute-force attacks [7].

Asymmetric Encryption: It is Public key encryption and two key encryption mechanisms. Those are public and private key. Both senders and revisers shares different key. More secure than symmetric encryption. Examples of this encryption algorithm are [5] [7]:

- RSA (Rivest-shamir-Adleman)
- Diffie-hellman key exchange
- Elliptic curve cryptography (ECC)
- Digital signature

Advantage of asymmetric encryption: No need of key exchanging, eliminating problem of key distribution, increasing security and provide digital signature Disadvantage of asymmetric encryption: speed that means less speed than secret key encryption. Hybrid encryption: Mode of encryption that inherits the best feature of both encryption systems. It is the combination of symmetric encryption and asymmetric encryption, but more strength in speed and security.

V. Proposed Work System

The proposed algorithm is the combination of (AES, RSA and SHA-1) and using this three algorithm to enhance security and privacy telehealth record over cloud computing.

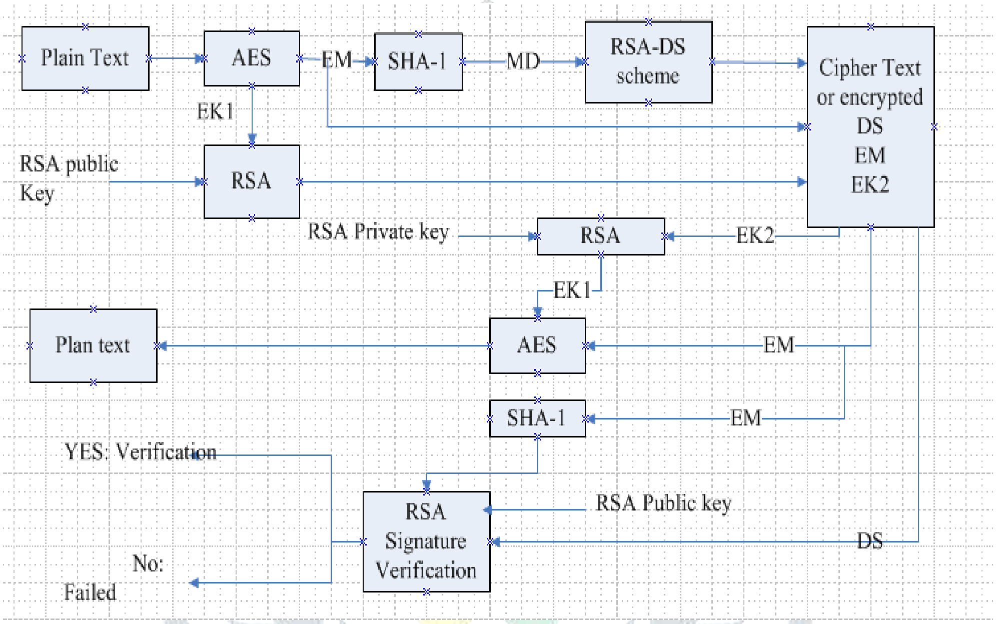

Figure 5.1. proposed Algorithm diagram

VI. PROPOSED WORK ALGORITHM

Many security models have been presented for cloud computing health care system, but this paper focus on store forward model of exchange data protection. Due to this reason we proposed hybrid cryptographic Encryption system that protects the stored data privacy and security [5] [7]. In this proposed system we use combination of symmetric and asymmetric algorithms AES and RSA with the authentication technique of hash function to encoding the cipher text and security key.

Since each algorithm has its own limitations, in order to decrease these limitations we prosed the combination or hybrid of algorithms. While combining these algorithms we focus on security and privacy of data stored in cloud storage specifically health record since it is very critical data. Encryption process of proposed algorithm is as listed below:

Step-1: The AES key “K” is choose from key size of 128,192 and 256 bit

Step-2: Using AES algorithm encrypt the Plain text (Pt) by above selected key
Step-3: (Pt) Plain text encrypted by AES and generates (EM) Encrypted Message
Step-4: AES key is encrypted by RSA algorithm and generates Encrypted Key (EK)
Step-5: Cipher text (EM) with SHA-1 algorithm generate message digest (MD)
Step-6: Digest message signed with RSA to generate DS(digital signature)
Step-7: EM, EK and DS send over network.

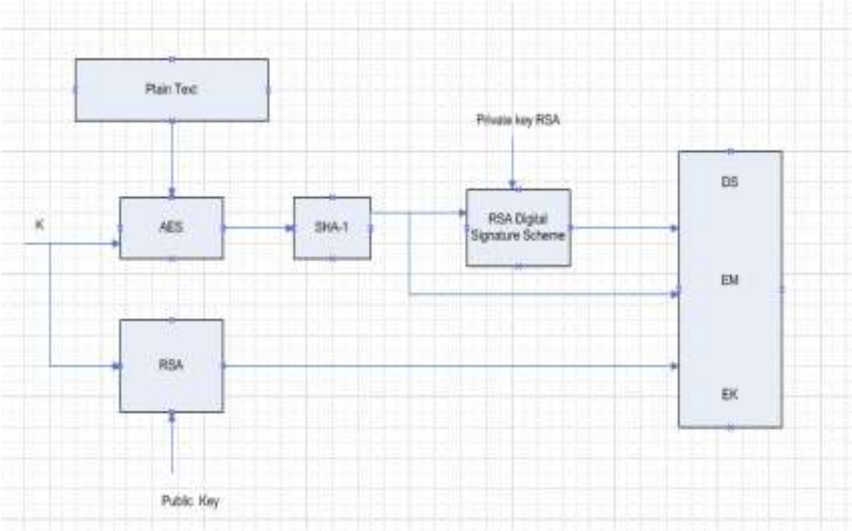

Figure 6.1 Encryption process

The encrypt file is sent to network and stored in cloud storage. In the time of need to reuse the data we have to decrypt that data. Decryption process of proposed algorithm is follows:

Step-1: Using AES algorithm encrypt key (EK) is decrypted by RSA algorithm and generate key (K)
Step-2: Encrypted message (EM) is decrypted by AES algorithm using key K to generate plain text
Step-3: message digest of encrypted message EM is computed with SHA-1 and generate message digest (MD)
Step-4: Digital signature is verified by RSA algorithm by using public key and produce digital signature (DS)

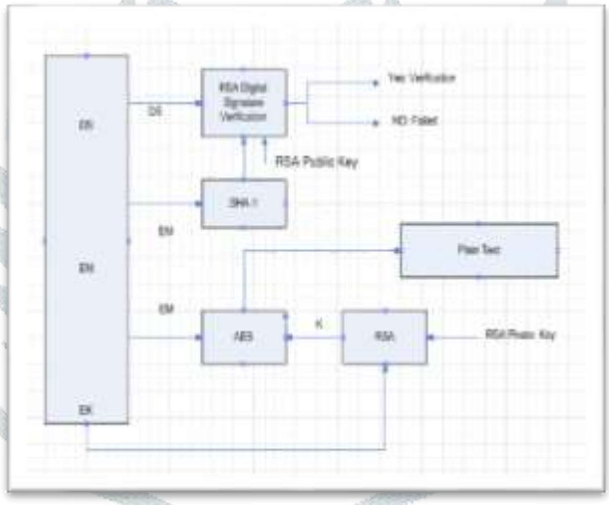

Figure **6.2** Decryption process

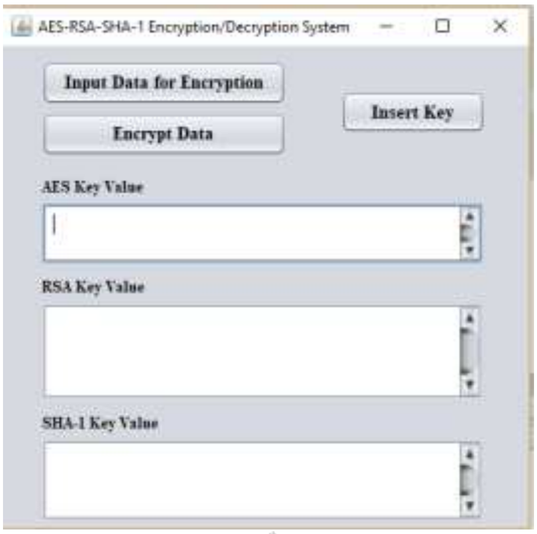
AES-RSA-SHA-1 Encryption/Decryption System
Input Data for Encryption
Encrypt Data
Insert Key
AES Key Value
RSA Key Value
SHA-1 Key Value

Figure 6.3 GUI of the proposed system that illustrates encryption process

VI. Result

As we have analyzed in this study paper, rather than using single encryption/decryption algorithm using hybrid is better in the case of security and privacy. In our proposed system we used hybrid encryption that the combination of three algorithms, AES, RSA, SHA-1. The main reason why we motivated to use this hybrid algorithm is because these algorithms have many disadvantages. The file encrypted using AES can be easily attacked by brute force. To reduce such attacks we used RSA algorithm which is mainly used for transporting key over untrusted network, SHA-1 for authentication purpose, and digital Signature (DS) with RSA is used for verification. Finally, by using hybrid or combination of those three algorithms is best for security of health that transmits over untrusted network and stored on cloud computing with improved security and privacy.

VII. Conclusion

The Cloud Computing is newly arising paradigm offers service for healthcare record systems in storing data which needs high security and privacy. In this paper we used combined three encryption algorithms AES, RSA and SHA-1. Then we developed the proposed system by using advantage of each three algorithms that build high security privacy system. Thus, we conclude that using hybrid algorithm gives us the most secure and private cloud storage that the customers do not afraid to store the health records on cloud. Future work we will eliminate twice use of RSA algorithm for decreasing complexity and time consumption of the system.

References

[1] Rizwana Shaikh , Jagrutee Banda, Pragna Bandi, “Securing E-healthcare records on Cloud Using Relevant data classification and Encryption” , International Journal Of Engineering And Computer Science ISSN: 2319-7242, Volume 6 Issue 2 Feb. 2017.

[2] G. Rathi, Abinaya. M, Deepika. M¸ Kavyasri. T, “Healthcare Data Security in Cloud Computing” IJIRCCEJournal, Vol. 3, Issue 3, March 2015.

[3] Aruna Devi. S, Manju.A, “ enhancing security features in cloud computing for healthcare using cipher and inter cloud”, IJRET, Volume: 03 Issue: 03 | Mar-2014

[4] Mr. Prashant Rewagad ,Ms.Yogita Pawar “Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption”, International Conference on Communication Systems and Network Technologies,IEEE explore , 2013

[5] Johann VINCENT Wei PAN and Gouenou COATRIEUX , “Privacy Protection and Security in eHealth Cloud Platform for Medical Image Sharing” IEEE explore, March 21-24, 2016

[6] Zhifeng Xiao and Yang Xiao,” Security and Privacy in Cloud Compting”, 2nd International Conference on Advanced Technologies for Signal and Image Processing ATSIP'2016 , March 21-24, 2016, Monastir, Tunisia

[7] Mr.Tejas P.Bhatt*1, Asst. Prof. Ashish Maheta#2,, “Security In Cloud Computing Using File Encryption”, International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 9, November- 2012.

[8] Akshay Arora, Anmol Rastogi, Abhirup Khanna, Amit Agarwal , “Cloud Security Ecosystem for Data Security and Privacy”, IEEE explore , 2017

[9] Rajkumar Buyya, Christian Vecchiola,S.Thamarai Selvi. Mastering cloud computing; McGraw Hill Education (India) Privat limited P-12,Green park Extension, New Delhi 110 016

[10] William stalling “Cryptographic and Network security, principle and practices”,4th Ed, November 16,2005