Family Medicine & Medical Science Research

Arun et al., Fam Med Med Sci Res 2015, 4:5
DOI: 10.4172/2327-4972.1000189

Research Article Open Access

Privacy of Health Information in Telemedicine on Private Cloud

Vanishree Arun[1]*, Padma SK[1] and Shyam V[2]

[1]Department of Information Science and Engineering, Sri Jayachamarajendra College of Engineering, Mysuru 570006, Karnataka, India
[2]Managing Director, Forus Health Pvt. Ltd, 2234, 23rd cross, BSK II stage, Bengaluru 560070, Karnataka, India

Abstract

Telemedicine involves many people at many levels with potential access to health records or medical data or the health details of a particular person. Privacy and security have always been an issue in telemedicine. In order to overcome this problem, cloud has been adopted to store and securely access data. Cloud offers a way to allow medical data and images to be transferred from patient to medical clinicians providing security. But individual patient data is not provided with privacy when it is outsourced to public cloud. In this paper, using a case study of screening the masses for early detection of non-communicable diseases at Sri Kshetra Suttur, privacy is built into telemedicine or mobile health care system with the help of the private cloud. Efficient key generation, Encryption, Decryption and analysis of health data misuse by authenticating authorized Clinicians to access patient records using Paillier Cryptosystem and Searchable Symmetric Encryption are some of the salient features introduced in this paper.

Keywords: Telemedicine; Cloud; Searchable Symmetric; Encryption; Paillier cryptosystem; Privacy

Introduction

Telemedicine helps in bringing health care access to remote locations. It enables the clinicians to evaluate, diagnose and treat patients remotely using the Information and Communication technology [1]. In order to make telemedicine effective, private cloud is used which offers services to both the sender and the receiver two-way communication. Since telemedicine relies on cloud for communication, it suffers from security and privacy issues. Therefore in our system privacy into mobile health care system with the help of the private cloud is built with efficient key management, privacy-preserving data storage, and retrieval, especially for retrieval at emergencies.

Relation between information society and surveillance society is a driving force for social and technology development. Society is becoming increasingly dependent on advanced technology in urban areas. Telemedicine adoption in connecting rural areas with the urban clinicians helps in generating of an open environment where clinician intervention is immediate which saves time and money and medical costs. Though existing telemedicine offers some safeguards in providing security to patient records, it cannot stop people from misappropriating medical records for various malicious reasons. This is a threat to healthcare practice. Technical challenges are always an issue. Effective bandwidth resources are essential to establish connectivity which was a great challenge in remote areas. Now since most of the rural places are well-networked, efficient telemedicine is ensured. In this study an effort is made to integrate telemedicine and privacy of individual patient record to ensure patient and clinician safety.

To provide affordable healthcare to the rural masses and to connect rural health data to the urban clinicians for immediate intervention, a project called "For Care" was launched at Srikshetra Suttur, Nanjangud Taluk, Mysuru to screen the masses for early detection of non-communicable diseases like Diabetes, Hypertension and Obesity. A Tablet was given to the rural health workers to record patient demographics using an app. Screening for Vitals like BP, Sugar, etc, was done by the health workers and eye screening was done by a technician at the primary healthcare centre, Suttur, using a hand held device called 3-Nethra. These values were recorded on the tab. A database repository is maintained on the cloud with security. Once the patient records are entered onto the tab, they are synced with the cloud to update the database. The anterior and posterior fundus images of eyes from 3-Nethra are also forwarded to the cloud. Simultaneously the record or image is forwarded by the health worker by selecting one of the disease-related clinicians at JSS Hospital, Mysuru, for intervention. The diagnosis of the clinician is sent back to health worker who alerts the patients about Physician Intervention or Secondary care referral. This is triggered from observed parameters in the screening phase by the clinician.

Here both Private cloud and Public cloud are used. When the patient record is synchronized with the cloud, medical details are stored in the private cloud. The stored data can be accessed and the results can be retrieved from public cloud. So it is understood that the storage, retrieval and computation tasks are performed by the cloud and light weight tasks for example uploading the data are done by the users and clinicians.

Paillier Cryptosystem algorithm is used to encrypt and decrypt patient records, where it allows the data to be stored on the remote server. Searchable Symmetric Encryption (SSE) allows to search the encrypted documents.

Related work

Most of works on privacy protection for mobile health data emphasize on the formation plan [2-7].Identity-Based Encryption (IBE) has particularly been used in simple role-based cryptographic access control [8]. Medical Information Privacy Assurance (MIPA) has given importance to e-health and medical information privacy, and the privacy violation facts that resulted from technology [5]. MIPA was used to develop health information system, in which individuals can protect their personal information.

Shruthishree et al propose encrypted cloud data search by securing conjunctive keyword ranked search [9-12]. Patient-Controlled Encryption (PCE) was proposed by J. Benaloh et al. where

***Corresponding author:** Dr.Vanishree Arun, Department of Information Science and Engineering, Sri Jayachamarajendra College of Engineering, Mysuru 570006, Karnataka, India, Tel:0094256348; E-mail: vanishriarun@gmail.com

Received October 08, 2015; **Accepted** November 24, 2015; **Published** November 30, 2015

Citation: Arun V, Padma SK, Shyam V (2015) Privacy of Health Information in Telemedicine on Private Cloud. Fam Med Med Sci Res 4: 189. doi:10.4172/2327-4972.1000189

health-related data are fragmented into a ladder of smaller pieces of information which are encrypted using the key which the patient will have control [10]. Ruj et al. proposes verification of authenticity of the user by the cloud by concealing the identity of the user and by allowing only authenticated users to decrypt the uploaded information thus preventing replay attacks [13-15]. Melissa Chase et al. proposed a solution by using Attribute based encryption to protect the users' privacy and by deleting the central authority [16].

The previous research works failed to address the challenges in data privacy, we aim to tackle in this paper cryptographic mechanisms for privacy-preserving on cloud.

Existing system

In the existing system of telemedicine incorporated in the project the records are transferred directly from health worker to clinician and back from clinician to health worker from private cloud with security. Individual records on the public cloud do not have privacy.

Proposed system

A Cloud is created as a repository and maintained at Forus Health Pvt. Ltd., Bengaluru, which is used for private cloud services which intern uses the infrastructure of the public cloud providers (e.g., Amazon, Google). When the health worker synchronizes patient records with the cloud, they are stored on the private cloud. When a particular clinician is chosen by the health worker, the record is searched and stored on the public cloud.

The activity starts once the registered user uploads the patient file. The file will be stored in the private cloud. The file includes medical data and images of various tests conducted of the patients related to their health conditions. Now the health data once uploaded, the data has to reach the clinician. To make it possible, next process is to view the data being uploaded, after viewing the data, a data key will be provided. The data key is generated in a sequential order. The data key is a secret key that is provided so that the data is secured. SSE algorithm is provided to generate the key so as to protect the data. Once this is done the final step that is performed by the user is to search for the specialized clinician requesting for treatment, the request will be sent to the clinician who has been requested for the treatment. Now the clinician will look into the data which is possible only when the data key is also shared by the user. Hence the clinician can view the data that is uploaded by the patient. All the information are stored in the private cloud.

When the patient record is entered onto the tab, and when it is synchronized with the cloud, each record in the form of a file will be encrypted and forwarded to the selected clinician. When the clinician downloads the file using the key provided, the file is decrypted. The encryption and decryption of the patient file are done using Paillier Cryptosystem.

The clinician writes the remarks in the field provided in the app and send the diagnosis and treatment back to the user as shown in Figure 1.

The Admin who logs in to the public cloud will have the ability to check only the auditing details of the users, and the basic details of the clinician. If the admin tries to access the medical data of the patients, a data key will have to be present to view. But, when the admin requests for a data key, a data key will not be provided instead a message will be displayed saying that the medical data can be viewed only by the clinicians.

Algorithms for key generation, encryption and decryption

Searchable symmetric encryption (SSE): when the patient records are synced with the cloud, SSE allows these encrypted records to be stored on remote server providing privacy. SSE also helps in searching the encrypted records [12].

SSE consists of the following steps with corresponding algorithms:

- Step 1: Generation of secret key. When each patient record is synced with the private cloud, the record is stored in a file and a key is generated to initialize the system.
- Step 2: Building records and Indexing. For a set of patient records, indexes are built, through which records can be searched.
- Step 3: Generation of corresponding trapdoor for the keywords of interest given by the clinician as an input search query.
- Step 4: When the clinician sends a query request to the cloud, a search for the file is performed on the index built in Step 2 with

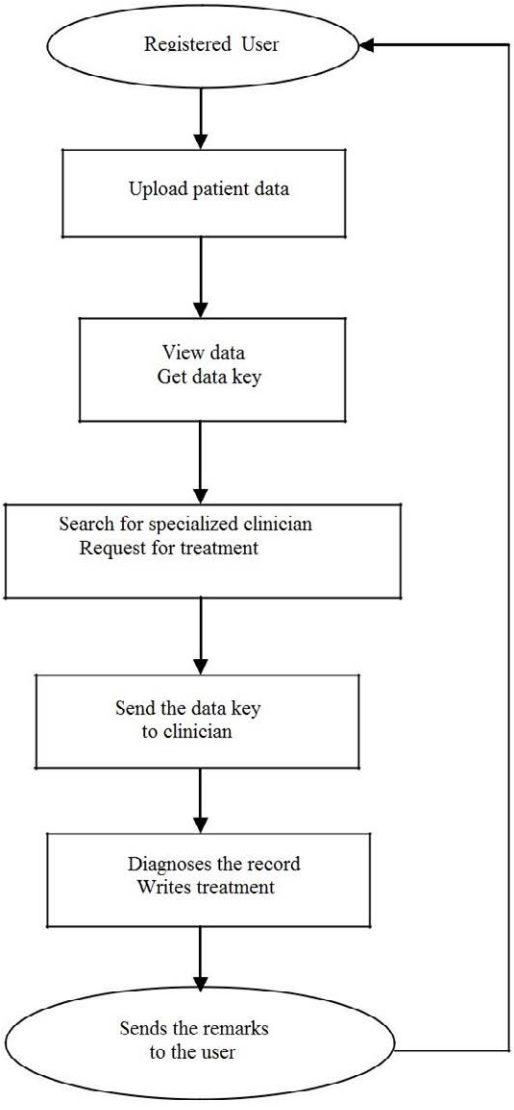

Figure 1: Flowchart of the system.

the help of trapdoor in the remote server. The output will be the list of files with similar keywords.

Algorithm to setup symmetric search encryption

- Begin
- Input : Upload patient file P using the app on tab ; K = KeyGen(a) ;

Security parameter a; Secret key K is generated ; I = BuildIdx(P,K) ;

Records are searched based on I; Tw = Trapdoor(K,w);

Compute trapdoor for keyword w; Search(I,Tw);

Search for records with Index I and Trapdoor Tw;

Output: List of files with keyword w.

End

Paillier cryptosystem: To securely share a patient record or an image between patient and clinician an additive homomorphic property of public key cryptosystem such as Paillier Cryptosystem is used. Asymmetric cryptosystem of Paillier is applied for encryption of patient records/ images. Due to additive homomorphic property of Paillier, addition operation over the plain text will give same result as multiplication over ciphered text. Extraction of record/image is possible only if the individual records/images are available [11].

Paillier cryptosystem algorithm

1: Select two large primes, p and q.

2: Calculate the product n=p x q, such that gcd (n,Φ(n)) = 1, where Φ(n) is Euler Function.

3: Choose a random number g, where g has order multiple of n or gcd (L(gλ mod n2), n) = 1, where L(t)= (t-1) / n and λ(n)=lcm(p-1,q-1).

4: The public key is composed of (g, n), while the private key is composed of (p,q,λ).

5: The Encryption of a message m< n is given by: c=gmrn mod n2

6: The Decryption of ciphertext c is given by: m=(L(gλ mod n2)/L(gλ mod n2))mod n

Homomorphic encryption:

$$E(x \otimes y) = E(x) \oplus E(y)$$

The generalized additive homomorphic property of Paillier encryption [13] is

$$\left(\prod_{i=1}^{l} E(m_i)\right) = E\left(\sum_{i=1}^{l} m_i\right)$$

Encryption: Figure 2 depicts the Encryption method where encryption of image is considered. The original image is encrypted and a scrambled image is obtained after the implementation of Paillier algorithm.

Decryption: Figure 3 depicts the Decryption method where scrambled image is decrypted back to the original image implementing Paillier algorithm onto Tablet. Patient profile and measurements are entered onto the Tablet by Mobile Health worker as in Figure 4.

B.3-Nethra screening: Eye screening is done using a hand-held device called 3-Nethra. Posterior and anterior Fundus images are captured and forwarded to cloud to store. The Clinician/doctor accesses and send diagnosis to the user as depicted in Figure 5.

Telemedicine with privacy: The input provided for this project is based on the roles present in the system, the roles are the users/health workers, the clinicians and the admin. The input at the time of log in provided by the user is that the basic demographic details at the time of registration and the username and the password, clinicians provide username and password whereas admin provides username and password. Inputs which are provided by the users and the clinicians are stored in the private cloud and the input provided by the admin is stored under the public cloud as in Figure 6.

Implementation

App Development: An app with fields for patient profile (Historical, Behavioral, Environmental) has been developed and loaded the processing starts from the user where the user uploads the patient record/ image as in Figure 7. A data key will be generated for the uploaded record.

The patients records/images and the clinicians log are on the private cloud. After the registration User will log on to the private cloud,

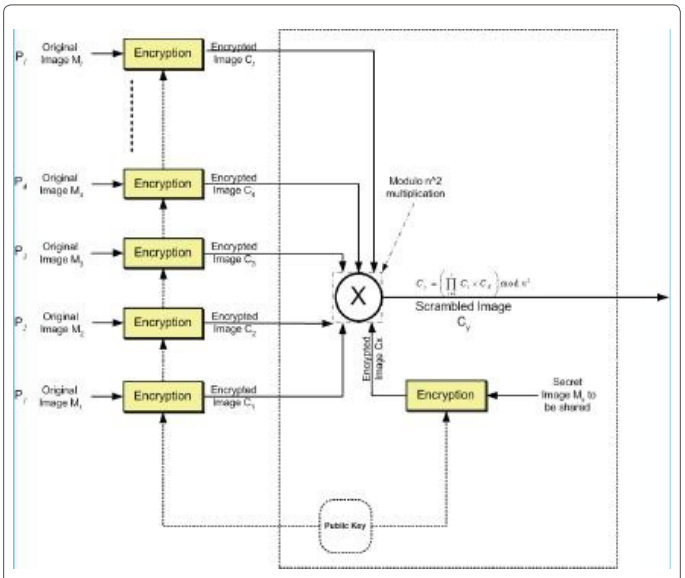

Figure 2: Encryption method.

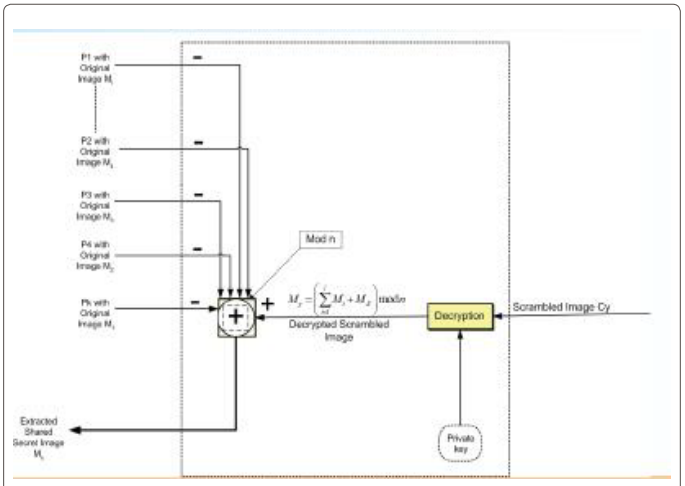

Figure 3: Decryption method.

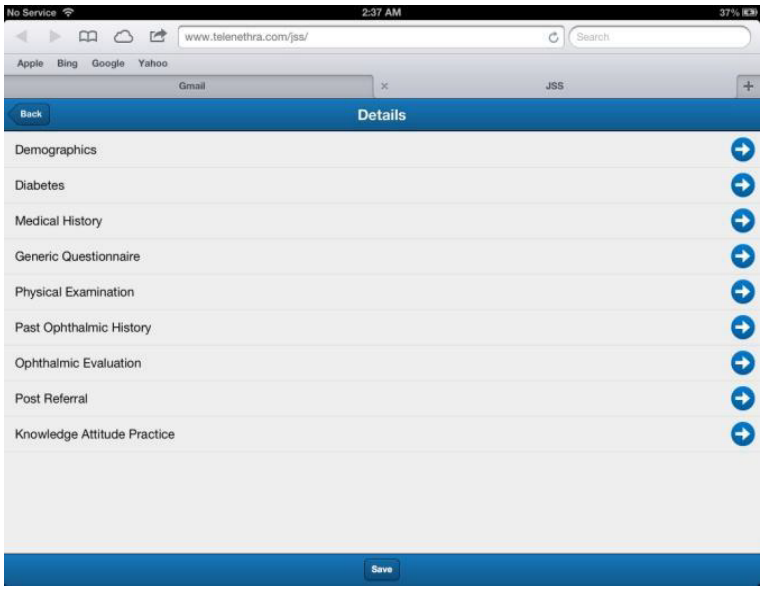

Figure 4: App from which medical details are entered onto tab.

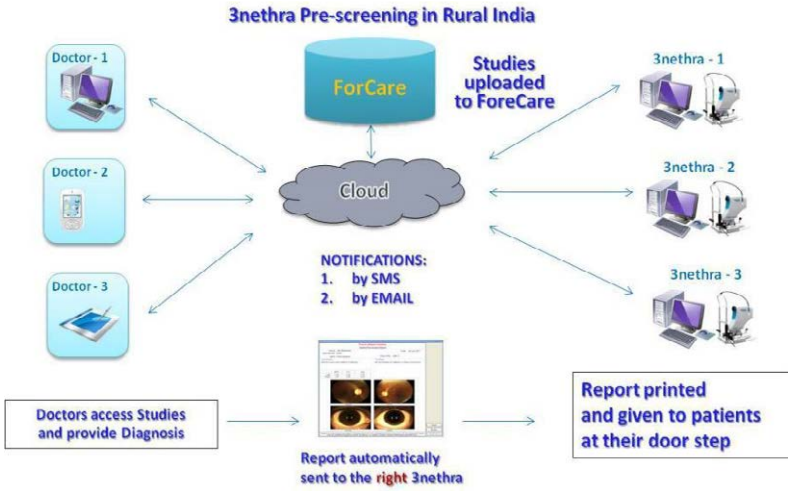

Figure 5: For Care Project : Pre-screening using 3-Nethra.

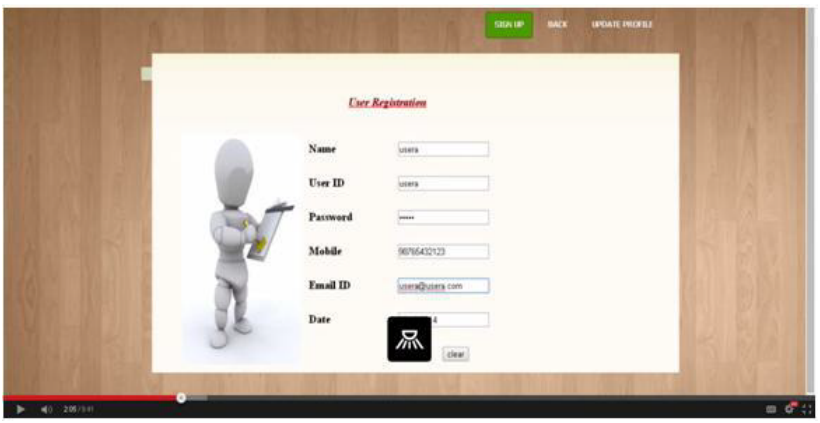

Figure 6: User registration screen.

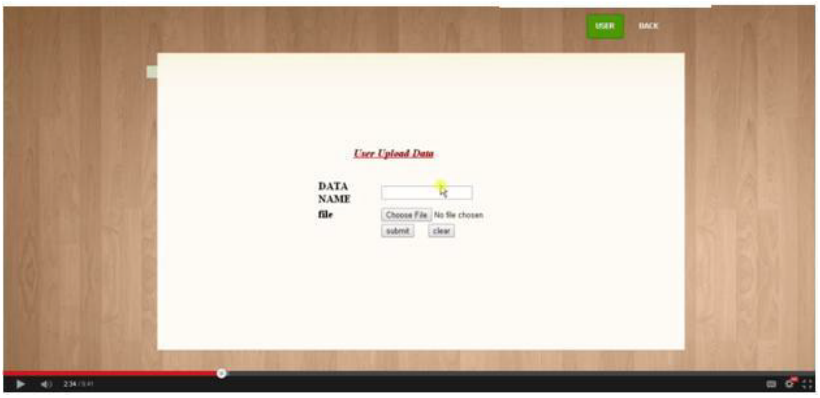

Figure 7: The user uploading the data.

Figure 8: After uploading the data the data key is been provided for the user.

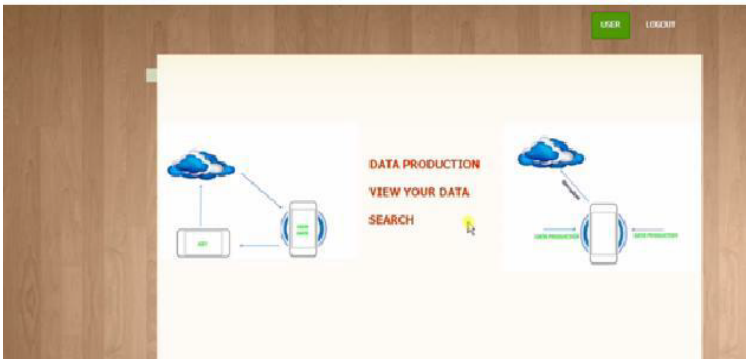

Figure 9: The 3 options present for the user, uploading, viewing the data and searching for specialized clinician.

upload the patient record/image, the user is provided with a secret data key for privacy, the data key is provided for maintaining the privacy of the medical data that has been uploaded as in Figure 8.

Once the clinician is selected, the clinician will view the data that has been uploaded using the key provided by the user as in Figure 10. Not every clinician in the telemedicine group can view the data of every other user.

The uploaded data is been viewed by the user. Hence, after this process the user will have an option to search for the clinicians for diagnosis as in Figure 9. The clinician enters the secret key and accesses the patient record/image and writes action to be taken and forwards back to the user as in Figure 11.

The admin who logs in to the public cloud can only see as well as check the details of the users required for auditing but will not be able

Figure 10: The data key is provided to the clinician.

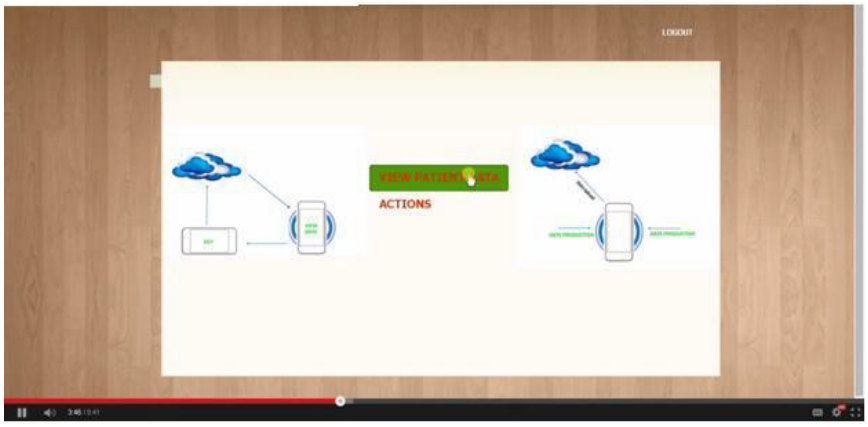

Figure 11: The clinician views the patient's data and enters the remarks in the Actions field.

Sl.No	Test cases	Test data	Results in existing model	Results in proposed model
1.	Sign_up screen for user	Same user with different username and password	Fail- no authentication for demographic details	Pass, cloud provides authentication for demographic details
2.	Login screen	Different user with same username and password	Fail-no authentication for demographic details	Pass, cloud provides authentication for demographic details
3.	File upload	No specific clinician, any random clinician view the health data	Fail-no authentication for patient record / image	Pass, cloud provides authentication for patient record / image
4.	File view	Random user can view the file uploaded	Fail- no authentication	Pass, cloud provides authentication
5.	Basic details and patient record / image	Any user and any clinician can see, other basic details and patient record / image	Fail- no authentication	Pass, cloud provides authentication,where as clinician views patient record / image and admin will view basic details

Table 1: Test results of existing and proposed model.

to see the patient records/images. The admin will also able to check the details of the clinicians.

Performance discussion

Some of the test results of existing and proposed model are shown in the Table 1. The existing system failed in authentication which was overcome by our proposed system. Thus our system resulted in an effective telemedicine with security as well as privacy to patient records and images.

Conclusion

By encryption and decryption of patient record/image applying Paillier cryptosystem and Searchable symmetric algorithm, the records/images are encrypted and indices are stored on the cloud. The clinician can access data by using the key provided by the user and decrypt. An analysis of health data misuse by authenticating authorized Clinicians to access patient records is done. If anyone who is not an authorized user tries to access or modify the patient records / images on cloud, an alert message is sent to the authorized user. Since privacy and analysis for misuse of data are provided to patient records and images, the efficiency of the overall system is increased.

Acknowledgment

We would like to thank Doctors from the Departments of Community Medicine and Ophthalmology, JSS Hospital, Mysuru, Karnataka, and Staff of Primary healthcare centre, Suttur, Karnataka for their constant support in the execution of this project and for their valuable comments and helpful suggestions.

References

1. www.globalmed.com/additional-resources/what-is-telemedicine.php
2. U.S. Department of Health & Human Service, Breaches Affecting 500 or More Individuals (2001) [Online].Available:http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationr ule/breachtool.html
3. Ray P, Wimalasiri J (2006) The need for technical solutions for maintaining the privacy of EHR. Conf Proc IEEE Eng Med Biol Soc 1: 4686-4689.
4. Mont MC, Bramhall P, Harrison K (2003) A flexible role-based secure messaging service: Exploiting IBE technology for privacy in health care. presented at the 14th Int. Workshop Database Expert Syst. Appl, Prague, Czech Republic.
5. Ateniese G, Curtmola R, de Medeiros B, Davis D (2002) Medical information privacy assurance: Cryptographic and system aspects. presented at the 3rd Conf. Security Commun.
6. Zhang L, Ahn G J, Chu BT (2002) A role-based delegation Frame work for healthcare information systems. in 7th ACM Symp. Access Control Models Technol, Monterey, CA, USA 2: 125–134.
7. Zhang L, Ahn G J, Chu BT (2003) A rule-based framework for Role based delegation and revocation. ACM Trans. Inf. Syst. Security 6: 404–441.
8. Boneh D, Franklin M (2003) Identity-based encryption from the Weil pairing. Extended abstract in CRYPTO 2001. SIAM J. Comput, 32: 586–615,
9. Sun J, Zhu X, Fang Y (2010) Preserving privacy in emergency response based on wireless body sensor networks. in Proc. IEEE Global Telecommun. Conf 3: 1–6.
10. Benaloh J, Chase M, Horvitz E, Lauter K (2009) Patient controlled encryption: Ensuring privacy of electronic medical records. in Proc. ACM Workshop Cloud Comput. Security 6: 103–114.
11. Naveed ISLAM, William PUECH, Robert BROUZET (2003) How to Secretly Share the Treasure Map of the Captain?
12. Shruthishree MK, Prasanna Kumar RS (2015) Secure Conjunctive Keyword Ranked Search over Encrypted Cloud Data. International Journal of Computer Science and Information Technology Research.
13. Michael Johnstone (2012) Cloud security: A case study in telemedicine. Australian eHealth Informatics and Security Conference.
14. Tobias Volkhausen (2006) Paillier Cryptosystem: A Mathematical Introduction.
15. Neame R1 (2013) Effective sharing of health records, maintaining privacy: a practical schema.Online J Public Health Inform 5: 217.
16. Melissa Chase, Sherman S, Chow M (2009) Improving privacy and security in multi-authority attribute-based encryption. 16th ACM Conference on Computer and Communications Security.