IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secure Identity-Based Data Sharing And Profile Matching For Mobile Healthcare Social Networks In Cloud Computing

Dr. Mrs. J. BHARATHI [*1], SYEDA KANEEZ E FATIMA [*2], KHATIJA ANAM [*3], SYEDA NABEELAH [*4]

[*1] Professor, Dept. of Electronics and Communication Engineering, Deccan College of Engineering and Technology
[*2] BE Student, Dept. of Electronics and Communication Engineering, Deccan College of Engineering and Technology
[*3] BE Student, Dept. of Electronics and Communication Engineering, Deccan College of Engineering and Technology
[*4] BE Student, Dept. of Electronics and Communication Engineering, Deccan College of Engineering and Technology

Abstract: The rapid growth of cloud computing and social networks is increasing day by day. So, if health care applications can deploy this technology, then the patients can store their privacy data in cloud storage and can share their feelings with other patients. For providing high security to patient health care records in this system we implemented a secure data distribution with an Identity-based cryptography technique. The patients can upload their electronic health records to cloud storage and share them to concern doctors with an identity-based encryption technique. The authorized doctors can access patient health records and respond to them securely. In this system we also use proxy re-encryption for doctors if they are not able to solve those cases then they can go with help of a specialist to cure it. While encrypted health care records sharing with specialists from doctors then no one can get the knowledge of those sensitive data. As well as patients can search for getting friends with their symptoms by profile matching technology securely.

Keywords— data security, health information management, profile matching, proxy re-encryption, fine-grained access control, Identity-based cryptography

I.INTRODUCTION

In cloud computing, the data owner can store huge of data securely for a long time. This sensitive data can access by authorized users remotely from anywhere. By using cloud computing the health care records can be shared with destination people through the network with help of a cloud service provider. The health providers can distribute these electronic health records to doctors secure which are shared by patients [1]. Now a day's people are spending their time on social networks so that they are willing to share their personal health records with doctors and specialists for better health causes. In this health care social network [2], the patients share their data like drugs and treatment through the cloud there is a chance to lose security. The data owners (patients) can't control the cloud server if the security is breached because the cloud is un-trusted. So that patients should encrypt their health records before outsourcing them to a cloud storage server and share with doctors and specialists.

The previous techniques provided many cryptography techniques like public-key encryption [3] which is a key pair-based technique, it can use a public key for encryption and a private

key for decryption. But using this cryptography technique the data can't share with multiple users at a time. In our system by using identity-based cryptography, patients can share their data with a group of doctors by applying an access policy on ciphertext data. In this system, the public key is the same for all users but everyone has their own private key with their user identity. The patients can make it ciphertext with help of a public key and share to consider doctors. The doctors can access the cloud data with help of their individual private keys. But these ciphertexts data can't share with a specialist so implementing proxy re-encryption can overcome this problem. The doctors can generate a re-encryption key with help of an attribute key and generate a ciphertext and sharing to a specialist.

II.RELATED WORKS

Zheng et al. [4] implemented an attribute-based encryption algorithm for encrypting the electronic health records as well as presenting access control over the data owner data which means they can control the cloud data by providing accessing permission. This kind of data can be accessed by those who can satisfy the access policy. Even using attribute-based encryption for providing fine-grained access control over EHRs, there is a drawback of heavy computation process while getting the encryption and decryptions stages.

Chen et al. [5] introduced the Identity-based signature technique for providing the security of health care records in cloud computing. In this system, patients can generate the signatures by taking input as EHRs and share to doctors through a cloud server. Then the doctors can verify the signature and access the data if it is valid or otherwise not accessed. There is a problem with group data sharing with a single signature as well as generating the signature for large size files there is a need to use large key size which leads to heavy computation cost for generating the signature.

The proxy re-encryption algorithm was implemented by Bleumer et al. [6] for secure data sharing in E-health cloud computing. The patients can encrypt the records and store them in the cloud later generate a re-encryption ciphertext with a re-encryption key and share it with delegators. It provided more security even cloud also cannot read the shared encrypted data. But patients are unable to provide access control of shared data which is losing access permission there are chances to access by everyone. To overcome the above all problems we proposed Identity-based encryption by sharing data with doctors as well as by proxy re-encryption doctors can share patient records specialists with securely by providing fine-grained access control.

III. SYSTEM IMPLEMENTATION

A. System Model:

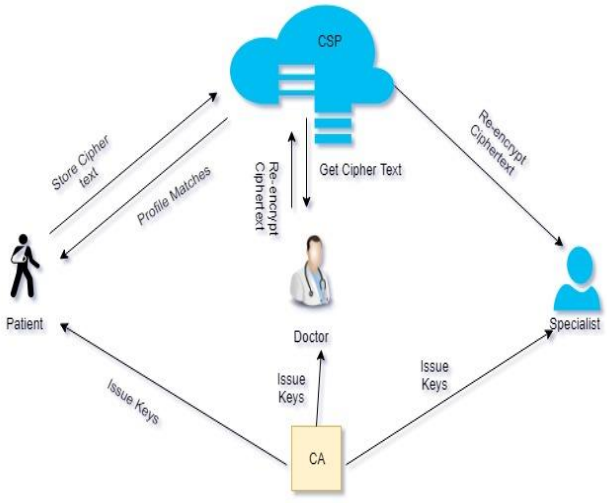

Fig.1 System model

Figure.1 depicts identity-based encryption with profile matching in cloud computing. This system can have five modules, each one can explain below.

CA: In this system central authority can generate attribute keys and private keys for patients, doctors, and specialists.

Data User (Patient): Here the patient can register into this system and get privileges keys to the central authority. The patient encrypts the electronic health records and outsources them into the cloud as well as they can share those records with authorized doctors. The patient can use profile matching protocol by searching with disease symptoms for making social relationships with their wills.

Physician (Doctor): In this system doctors also can register and get attributes keys and private keys from the central authority. The doctors can decrypt the patient's healthcare records and responses to patients with prescriptions. Sometimes they can share the patient's records with a specialist if they encountered a problem. Hereby using proxy re-encryption techniques doctors can securely share the records with specialists with access policy conditions.

Specialist: The specialist can get a private key by registering into this system which is generated by CA. The specialist can decrypt re-encryption data with their private key and assist doctors with advice.

CSP: The cloud service provider can monitor the data storage and it can pretend to be semi-trusted storage servers as well as they will respond to patient's profile matching requests.

B. Our proposed algorithm

Our proposed system of Identity-based encryption consists of the following algorithms:

SysInitializing:

This algorithm can take input as a system parameter $\emptyset$ and generate outputs a public key *PK* and master key *MK*.

Key Generation-1:

This algorithm inputs the public key *PK* and master key *MK*, the identity *ID* of patients, doctors, and specialists then it can generate the outputs as individual private key *SK*.

Key Generation-2:

This algorithm inputs the public key *PK* and master key *MK*, a set of doctor attribute *S* then it returns the outputs as attribute key *AK* for doctors.

Encrypt EHR:

This algorithm can take inputs public key *PK*, doctor's identities *U*, an access policy *T*, and the patient report *M* then it returns the ciphertext *CT* by applying the IBE algorithm.

Re-encryption Key Generation:

The algorithm can take inputs private key *SK* and doctors attribute key *AK* with identity *ID*, system public key *PK*, and a specialist's identity *IDs* then it returns a re-encryption key RK.

Re-Encryption:

The algorithm inputs the re-encryption key *RK* of a doctor, public key *PK*, and an initial the ciphertext *CT* then It returns a re-encrypted ciphertext CT'.

Decryption EHR (Doctor):

The algorithm inputs a secret key *SK* for a doctor, a public key *PK*, and an initial the ciphertext *CT*

then it returns the electronic health records *M* if the doctor's attributes satisfy the access policy *T*, otherwise, they were denied to access that report.

Decryption EHR (Specialist):

The algorithm inputs a secret key *SK* for a specialist, re-encrypted ciphertext *CT′* then it returns the patient report *M* if the specialist's attributes satisfy the access policy *T*, otherwise, they were denied to access that report.

Decryption EHR (Patient):

The algorithm inputs a secret key *SK* of a patient, and the doctor responded ciphertext *DCT* then it returns the patient's precautions reports and the patient can download it.

Profile Matching:

In the profile matching methodology, the patient can search with the symptom's keywords like fever, cold, etc with the cloud server then it will return patient's details whose symptoms are matched with searching keywords.

IV. EXPERIMENTAL RESULTS

Fig.2. System Setup for Public & Mater key

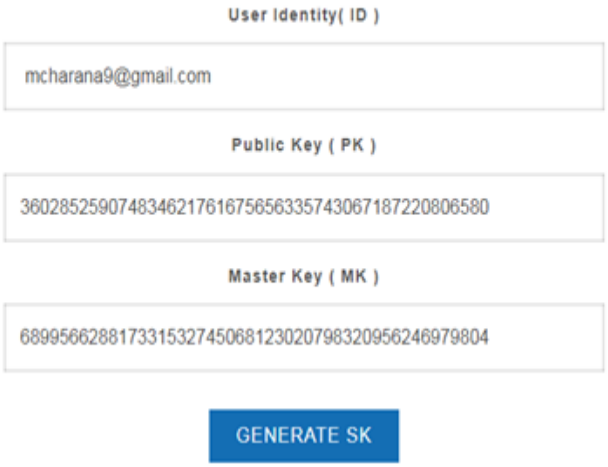

Fig.3 Private Key Generation for Patient, Doctor, and Specialist

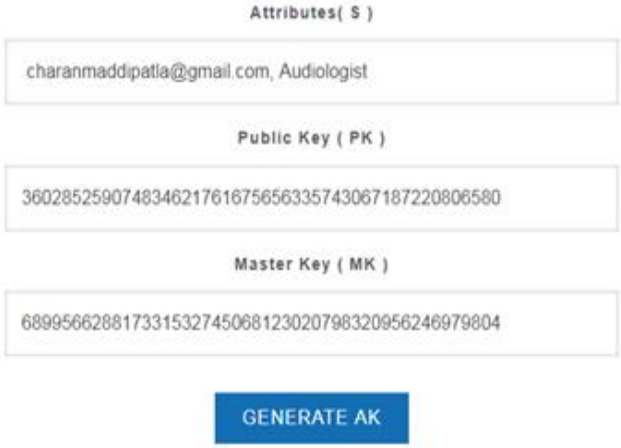

Fig.4 Attribute key generation for doctors

Fig.5 Health Records Encryption

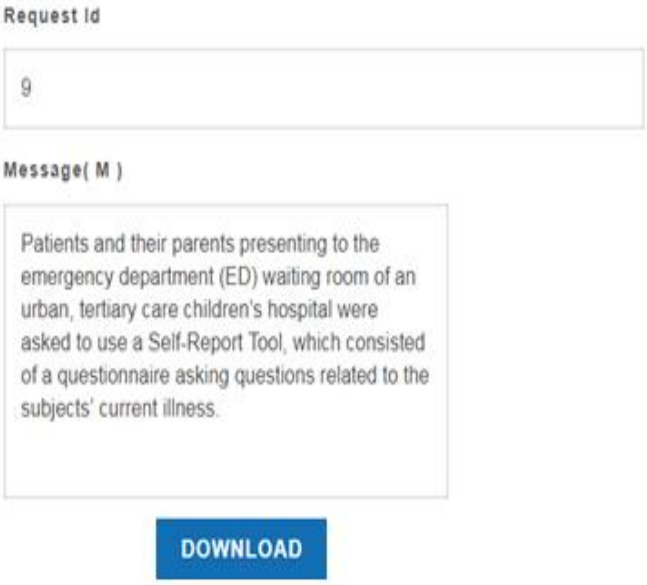

Fig.6 Health Records Decryption

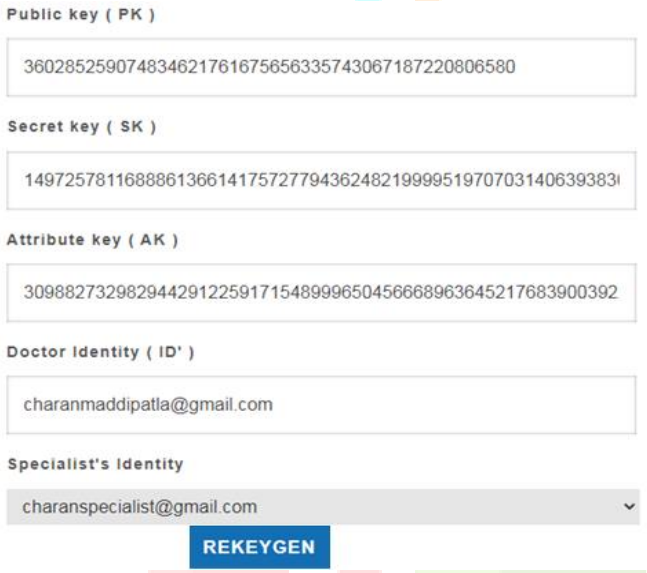

Fig.7. Proxy Re-enc key Generation

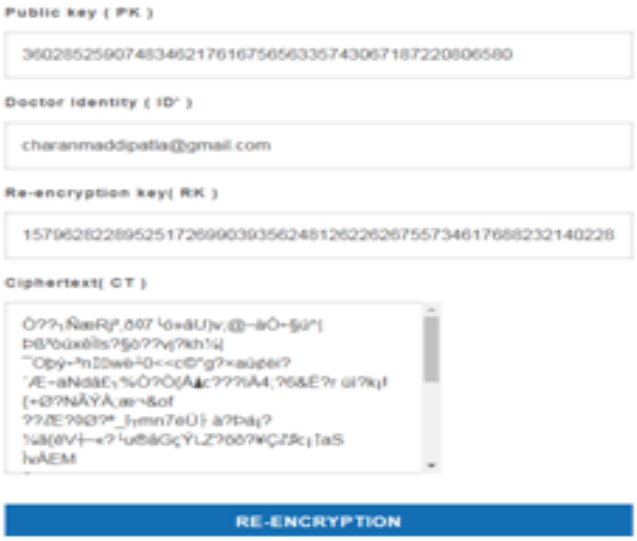

Fig.8 Proxy Re-Encryption

V. CONCLUSION

In this system, we proposed a secure identity-based cryptography technique and profile matching. We first apply the IBE algorithm which is allowed us to patient encrypt health care recodes and share to with a group of doctors securely. Later by providing a proxy re-encryption algorithm doctors can share the patient's sensitive data with a specialist by applying access conditions. Finally, by implementing profile matching, patients can make a social relationship by finding friends with disease symptoms. The proposed system results show the effectiveness of the system security.

VI. REFERENCES

[1] L. Guo, C. Zhang, J. Sun and Y. Fang, "PAAS: A privacy-preserving attribute-based authentication system for E-health networks," in Proc.32nd International Conference on Distributed Computing Systems, Macau, China, 2012, pp. 224-233.

[2] A. Abbas and S. Khan, "A Review on the state-of-the-art privacy-preserving approaches in the e-Health clouds," IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 4, pp. 1431-1441, Jul.2014.

[3] S. Ma, Q. Huang, M. Zhang and B. Yang, "Efficient public key encryption with equality test supporting flexible authorization," IEEE Trans. Inf. Forensic Secure., vol. 10, no. 3, pp. 458-470, Mar. 2015.

[4] M. Li, S. Yu, Y. Zheng, K. Ren and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Trans on Parallel and Distrib. Syst., vol. 24, no. 1, pp. 131-143, Jan. 2013.

[5] G. Li, C. Chen, H. Chen, F. Lin and C. Gu, "Design of a secure and effective medical cyber-physical system for ubiquitous telemonitoring pregnancy," Concurrency and Computation Practice and Experience, vol. 30, no. 2, pp. 1-16, Jan. 2018.

[6] M. Blaze, G. Bleumer and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proc. Advances in Cryptology - EUROCRYPT' 98, Espoo, Finla nd, 1998, pp. 127-144.