Double Protection Encryption Scheme for Secured Data Transmission

[1*]Dr.S.Muthusundari, [2]L.Sherin Beevi,[3]A.Nithya, [4]K.Gunasekaran,

[1]Associate Professor, Department of CSE, R.M.D. Engineering College,
Kavaraipettai, sms.cse@rmd.ac.in
[2]Assistant Professor, Department of CSE, R.M.D. Engineering College,
Kavaraipettai.
[3]Assistant Professor, Department of CSE, R.M.K.College of Engineering and Technology,
Kavaraipettai.
[4]Assistant Professor, Department of CSE, Panimalar Engineering College,
Chennai.
*Corresponding Author E-mail: sms.cse@rmd.ac.in

Abstract:

This proposed system introduces a new double protection data dividing and equal with system in cloud environment. This proposed system maintains the patient's encrypted medical reports to cloud data base with specification based distribute encryption (SBDI) technique, and it is to be shared to a consulting group in a sound and protective approach. It takes characteristic -based action on text data decryption mechanism, which empower the consultant to access the patient's record without discharging any users relevant information. Further, it provides a resume checkingsystemusing specification based distribute encryption that helps users to find consultation in a secured way, and attain their easy approved way on the protected medical reports.

Keyword*:* Secure data sharing, specification based distribute encryption, characteristic based action.

1. Introduction

The Health care in the online internet consultation isthe best way of connecting mobile phones with internet connection in the world. The day to day routine of daily care in the health facts is the improvement and possible to prevent from the diseases of users by the awareness of the health facets.This requires an urgent and needy in the currents trends in cloud computing environment for the patients care.The monitoring of healthcare system using mobile phones with internet connection shows the electronic health record of medical patient data (HER). However, to protect the medical reports lots of challenging safety measures is discussing to overcome the problemsin order to maintain a healthy and safety medical reports in the cloud storage system. In this proposed system, it introduces a double protection secure data divined with resume checkingsystem for MHSN in cloud storage environment. The patient's details are initially verified by the doctor. If the doctor can able to identify the problem once, then he will again encrypt the medical records and send to cloud for other specialist verification.Then it will be diagnosed by other specialists for request. For better experience, a chat box is extended between doctor and patient. This chat box can be created by doctor. If the doctor finds the provided information is not enough to diagnose the patient's problem, then the doctor needs the chat box to collect more information form the patient user.The record of medical history for each and every patient is maintained propoerly.

2. Literature Survey

2.1P. Xu, T. Jiao, Q. Wu, W. Wang and H. Jin,

This paper discussed the action based overspread duplicate decryption mechanism.They proposeda different approach of CIBPRE scheme with provable double encryption method. In this paper, they discussed on constant size record is protected and decrypted.

Y. Yang, H. Zhu, H. Lu, J. Weng, Y. Zhang and K. Choo

This paper is defined a computing based data dividend with chopped grain technique of encryption scheme.They implemented a new method for key transforming code generation in cloud concept. This approachis dealt with data splitting using the features of grain technique of access control mechanism for data confidentiality.

2.2 Q. Huang, Y. Yang and J. Fu

This paper focused on specification needs private data dividing with tested oriented proxy decryption process in online economic culturemedia. They demonstrated the usage of their scheme comparatively with other fine-grained data sharing for user's protection of their data. This system successfully implemented a cloud based secured transmission. The end users are more in this application.

3. Existing System:

3.1Resume checking in storage Media

Resume checking is asignificant way to identify the general issues between persons to persons. This will helpful to guide patient to get rid of the general problem issues of their health in a fast way. This system mainly focuses the security issues of the user'shealth reports. The basic details of the user's data are shared. Anyway for the double protection, the encryption and decryption process is concentrated

4. Proposed System

A. **Secure** specification based distribute encryption

This proposed system introduces a double protection specification based distribute encryption data sharing system for MHSN, it permits the users to outward their cipher text of medical reports to CDP with specification based distribute encryption technique, and share them to a group of consultants in a safe and protectivefashion. It includes fivemain attributes, they are as follows: final level authority, CDP, user, consultant and expert.

(1) Final level authority. The final level authorityonly initiating the proposed system and to generate the key attributes for the users.

(2) CDP. The CDP is called cloud database platform. It is only responsible for storage of patient's health record to the cloud and it acts as a duplicate for storage purposes

(3) User. The patient is acted as user of the system. They update the entire process byregister with their code words.

(4) Consultant The Doctors are the end users to view the details from the cloud and to decrypt the user'sencrypted medical history that resides in the CDP.

(5) Expert. The specialist are the one who could decrypt the ciphertext of their medical reports with the code word and then need suggestion from experts for prescription.

B. Back track of patient details and chat box

We provide each patient with unique id and thereby we can manage to track our past records. It's important as to proceed further we need to have track of previous records. It can be referred by doctors, if they need it for analyzing. If doctor needs to know further details about the patient, he/she can initiate a chat box. This can be initiated only by doctor and not by patient at any time. The chat box has application to upload pictures and information related to health issues.

5. Modules

5.1 Social Cloud

Social media is a one of speedy machine level description with built-in faithfulcommunications betweenend users and users. This virtual medium is used to createthe social media effects on real world entities. It only permits the users to interact, form inter connections and to share information with one another.

5.2Public and Secret Maintenance Steps

In this challenge the secret level threat is created for security purpose for the login purpose. The secret key is then confidentiallycreated for users login process. The final level security is developed for maintain the SK for each entity using the KeyGeneration idea algorithm.

6. Block Diagram

The block diagram of encryption scheme is depicted in the following **figure** .

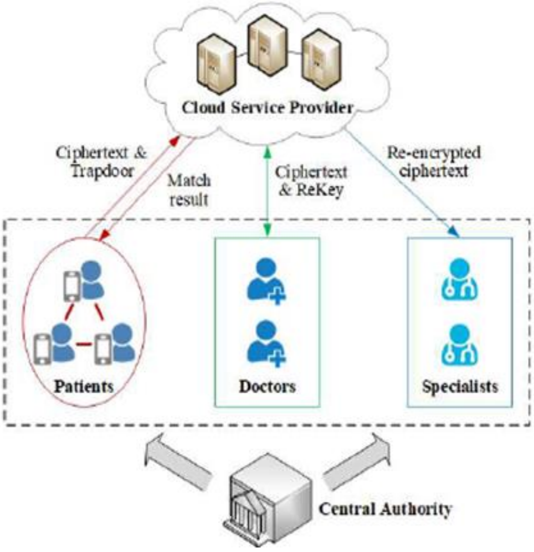


Figure 1. Encryption Scheme Block Diagram

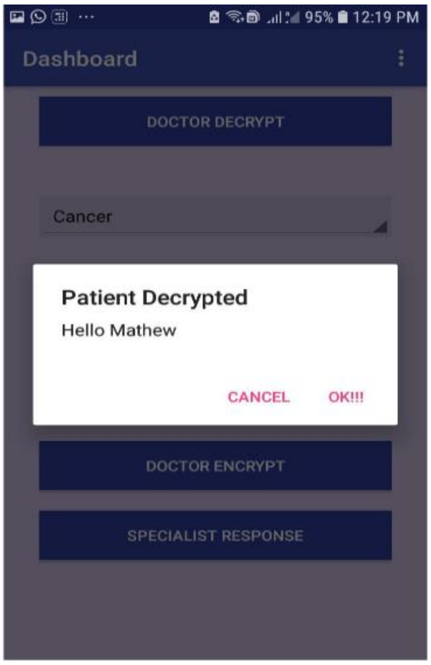
The figure is described the double protection of encryption scheme.In this proposed system, it introduces a new double protection datadividing and equal with systemfor MHSN in cloud system. The users can outward their cipher protectedmedical reports to cloud data base with specification based distribute encryption (SBDI) technique, and split it to a group of consultants in a safe way and protective fashion. It took acharacteristic -based action on text data decryption, which allows the doctors to view the preset actions in the rearranged data records.

7. Results and Disscussions

The proposed double protection encryption scheme has been implemented in Java platform. The sample coding has been listed here.

```
Packagecom.smart.isi_admin.secure.IBE.CentralAuthority;

Importjava.io.DataInputStream;

Importjava.io.IOException;

Importjava.math.BigInteger;

Importjava.util.Random;

Public class RSA {

BigIntegerpublic_key,private_key;

Private long public_key_temp;

PrivateBigInteger p;

PrivateBigInteger q;

PrivateBigInteger n;

PrivateBigInteger phi;

PrivateBigInteger e;

PrivateBigInteger d;

Privateintbitlength = 1024;

Private Random r;

String ID;

RSA (String ID) {

this.ID = ID;

public_key_temp = Math.abs(ID.hashCode());

r = new Random ();

p = BigInteger.probablePrime(bitlength, r);

q = BigInteger.probablePrime(bitlength, r);

n = p.multiply(q);

}
```

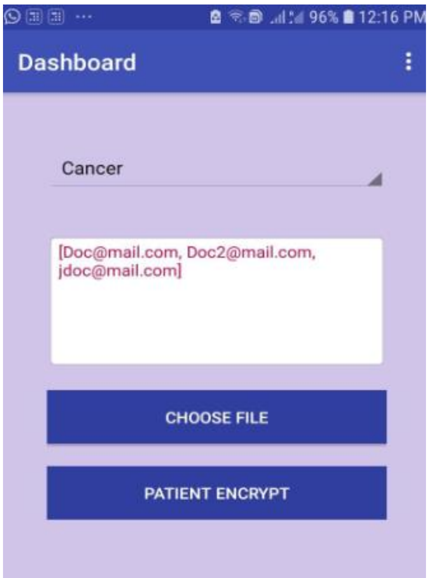
The result of the patients decrypted details are shown in the figure 2.



Patient Decrypted

Hello Mathew

Figure2. Patient Decrypted Details



[Doc@mail.com, Doc2@mail.com, jdoc@mail.com]

Figure 3. Patient Details

8. Conclusion

Securing medical data has become a tough task in recent times .Future hospitals will be managed through applications. Therefore, we took initial steps in making it secure and user friendly to patients. We provide diagnosis of disease by doctors based on their disease and doctor's qualification. We make it possible through attribute based condition. The information provided by patient is secured by IBBE technique. The information is encrypted and then it is broadcasted to cloud which contains a kind of doctors. As we said early, the patient details are given to corresponding doctor through a key. Only the doctor who holds the key can read the data. If he could diagnosis the disease, he will respond to it. If he needs still more data for analyzing, he can initiate a chat box. If he/she can't diagnosisthe disease, he will decrypt the data and transfer to cloud database platform (CDP). The key is again given for a specialist. As there involves double encryption, the data is more secure. Along with it we provide back track of previous health records.

References

[1] L. Guo, C. Zhang, J. Sun and Y. Fang, "PAAS: A privacy-preserving attribute-based authentication system for ehealth networks," in

Proc. 32nd International Conference on Distributed Computing Systems, Macau, China, (2012) 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, 18(4)(Jul. 2014) 1431-1441.

[3] C. Delerablée, “Identity-based broadcast encryption with constant size ciphertexts and private keys”, in Proc. 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, (2007) 200-215.

[4] J. Bethencourt, A. Sahai and B. Waters, “Ciphertext-policy attribute-based encryption”, in Proc. 2007 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, (2007) 321-334.

[5] M. Green, G. Ateniese, “Identity-based proxy re-encryption”, in Proc. the 5th International Conference on Applied Cryptography and Network Security, Zhuhai, China, (2007) 288-306.

[6] 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., 24(1)(Jan. 2013)131-143.

[7] M. Barua X. Liang, R. Lu and X. Shen, “ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing,” International Journal of Security and Networks, 6(2/3)(Nov. 2011) 67-76.

[8] S. Yu, C. Wang, K. Ren and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing”, in Proc. 29th Conference on Information Communications, San Diego, CA, USA, (2010) 534-542.

[9] Y. Liu, Y. Zhang, J. Ling and Z. Liu, “Secure and fine-grained access control on e-healthcare records in mobile cloud computing”, Future Generat. Comput. Syst., 78(Jan. 2017)1020-1026.

[10] Y. Yang, X. Liu, R. Deng and Y. Li, “Lightweight sharable and traceable secure mobile health system”, IEEE Trans. Depend. Sec Comput., Jul. 2017. [Online]. Available: https://doi.org/10.1109/TDSC.2017.2729556.

[11] Y. Yang, X. Liu and R. Deng, “Lightweight break-glass access control system for healthcare internet-of-things”, IEEE Transactions on Industrial Informatics, Sept. 2017. [Online]. Available: https://doi.org/10. 1109/TII.2017.2751640

[12] 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, 30(2)(Jan. 2018) 1-16.

[13] C. Tan, H. Wang, S. Zhong and Q. Li, “IBE-Lite: a lightweight identity-based cryptography for body sensor networks,” IEEE Transactions on Information Technology in Biomedicine, 13(6)(Nov. 2009) 926-932.

[14] X. Wang, J. Ma, F. Xhafa, M. Zhang and X. Luo, “Cost-effective secure E-health cloud system using identity based cryptographic techniques,” Future Generat. Comput. Syst., 67(Feb. 2017) 242-254.

[15] M. Blaze, G. Bleumer and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in Proc. Advances in Cryptology - EUROCRYPT' 98, Espoo, Finland, (1998) 127-144.

[16] T. Matsuo, “Proxy re-encryption systems for identity-based encryption,” in Proc. 1st International Conference on Pairing-Based Cryptography, Tokyo, Japan, (2007) 247-267.

[17] Y. Zhou, H. Deng, Q. Wu, B. Qin, J. Liu and Y. Ding, “Identity-based proxy re-encryption version 2: Making mobile access easy in cloud,” Future Generat. Comput. Syst., 62(Sept. 2016) 128-139.