International Journal of Engineering Technology and Management Sciences[IJETMS]

Website: ijetms.in Issue:2, Volume No.2, July-2018 ISSN: 2581-4621(Online)

A SCALABLE DECENTRALIZED ACCESSING OF HEALTH CARE DATA WITH IMPORVED PRIVACY OVER CLOUD HEALTH MONITORING SYSTEM

K.Arumugam[1], Dr.P.Sumathi[2]
[1]PhD Research Scholar, [2]Assistant Professor
PG & Research Department of Computer Science
Government Arts College, Coimbatore, Tamilnadu, India.

[1]aaruk.dpm@gmail.com
[2]sumathirajes@hotmail.com

***Abstract* — Cloud health monitoring (CHM) becomes the popular technology in real world where the number of users increased in number. It is one of the revolutionary approaches which enable patients to retrieve their health care information with reduced cost. CHM enables the patients to access and modify the data's that are stored in the cloud. CHM contains the sensitive information about the multiple patients where privacy becomes the biggest issue. In this research work, decentralized privacy preserved health care monitoring service is proposed which aims to reduce the burden of users and hospital management. In the proposed work, health care information will be gathered from the multiple users who are located in the different location. The anonymous data access control is enabled in the cloud where the users are distributed across multiple locations. Moreover, dynamic creation of cipher text class id's (used to differentiate the different blocks of data) is introduced to support the numerous amount of data that are received from multiple locations. However anonymous access of data over the decentralized server is most difficult process where there is no presence of centralized server. To overcome this problem a novel authentication process is introduced for the checking the verifiability for the unknown users who are located in different locations. The experimental tests were conducted to prove that the proposed methodology provides better result than the existing approaches in terms of improved privacy and scalability.**

***Keywords* — Cloud health monitoring, Anonymous patients, Decentralized server, Scalability.**

I. INTRODUCTION

Quick access to the health data will leads to an optimal health care service provisioning through which quality of life can be improved considerably [3]. It can save the life by providing timely treatment in medical emergencies. However, 24 hr/any place accessing of health care information through electronic devices will be more difficult process in which the more security violation may occur. This application significantly reduces the hospital occupancy such that patients with higher need of hospitals can be admitted immediately.

The research over a cloud computing are increasing more where the usage of cloud networks are increased in number [1]. Cloud health monitoring is one of the most popular applications in cloud computing which enables the users to store their health care information in the cloud server. The roles involved in the cloud computing are patients, hospital management (HM), emergency care unit (ECU) people, and cloud service provider (CSP). Hospital management is responsible for gathering the patient health care information from the patients are all getting treatment in their hospitals. Hospital management will take care of the sensitive data's that are gathered from the patients and will take necessary steps to prevent the data's from malicious activities. HM will store the health care information about the patients in the CSP. Patients will send requests to the cloud service provider in case of emergency along the symptoms message. The cloud service provider will transfer that message to the ECU people who are responsible for suggesting the proper treatment. ECU people will access the health care information of patients that are stored in the cloud server by sending the proper identification information to the cloud service providers. The CSP will authenticate the users before providing them access permission. The ECU people can take the proper decision by analysing the health care information and will send back the treatment data's for the CSP.

The main contribution of is given as follows:

1. Supporting the large amount of data's which are retrieved from the more number of users from different locations.
2. Implementing the decentralized computing network through which more number of users from different locations can make use of health care information in effective manner.
3. Provide an anonymized access control over the health care information that is stored in the cloud server to assure the privacy guarantee. The above contributions are achieved in this work by introducing the novel approach called the decentralized privacy preserved health care monitoring service through which one can access and give an health care suggestion for the patients who are in need to access it.

The organization of this work is given as follows: chapter 1 provides a detailed description about the introduction of health care monitoring services. Chapter 2 discusses the various previous researches that have been conducted to provide an efficient health care monitoring service. In chapter 3, contribution of this work is discussed in the detailed manner. In chapter 4 experimental tests results were compared with the previous studies to prove the wellness of proposed methodology. Finally in chapter 5, overall goal of this work is concluded.

II. RELATED STUDIES

Elaine Shi John Bethencourt et al., [2] discussed the way of querying the encrypted data's that are stored in the cloud. The accessing and make use of encrypted data's are the most difficult process where the information about the data's will be hidden from the users. To access the encrypted contents one need to submit their verification information to the users, so that the cloud service providers can authenticate for providing them access permission.

Xavier Boyen et al., [5] introduced the hierarchical identity based encryption, so that the privacy of the users cannot be leaked where the identity of the users have been used for the encryption of data contents. Hierarchical IBE will encrypt the data contents by using the multiple identity information which is collected from the multiple valid users. HIBE provides flexible way for the cloud service providers to authenticate the data contents that are stored in the cloud network.

Sushmita Ruj et al., [4] introduced a novel methodology for providing the access control for the data's that are stored in the cloud in the encrypted format. It provides a security where the data's that are collected from the various users will be encrypted before storing in the cloud server. The security is enabled where the access permission for the users are enabled only after verifying the identity information that are submitted by the users.

III. DECENTRALIZED PRIVACY PRESERVED HEALTH CARE MONITORING SERVICE

Cloud health monitoring is the most important application scenario in the real world environment where the patients make use of the electronic devices to acquire the health care advice for their ills without visiting hospitals. By doing so, burden of hospital environment can be reduced considerably and also the travelling burden and cost of the patients can be reduced. Emergency Care Unit is responsible for the taking the health care decision for the patients. ECU requires accessing the history of health care information about the corresponding patient for, making accurate decision for the patients ills from the symptom data's that are submitted by the users through electronic devices. However giving access permission for patients historical data will leads to privacy violation of the patients where the data may consists of the sensitive information about them which they don't want to share with others.

In order to support the multiple users who are located across multiple locations, in this work cloud server is decentralized where the multiple servers will reside in the every location. Thus no longer it is required to depend on the single server for getting data access permission. The authentications of the ECU people are done in the decentralized manner where there is no centralized server present to control the activities. Hospital management will buy some amount of resource from the cloud service providers to store the health care information of patients from which it will be shared with the ECU peoples. In the real world, the amount of information will be increased as the numbers of users are increased. In that case, data encryption will become the most complex issue.

The data encryption in the cloud environment is done by dividing the entire data into multiple blocks and encrypting them with unique cipher text class id's. The number of cipher text class id will be limited because of limited cloud storage. If the cloud server consists of n class id then the data will be divided into n blocks. It will lack form the performance where the dynamic growth of cloud data's are exist due to increasing number of users. To overcome this problem in this work, dynamic decision of number of cipher text class id's are introduced.

The overall flow of this research work is given as follows:

1. Decide the number of cipher text class id's
2. Give the access permission in the decentralized environment
3. Authenticate the users before giving them permission to access the contents.

These will be discussed shortly in the following sections.

A. Decide the Number of Cipher Text Class Id's: Health care information of each and every patient will be maintained by the hospital management. The hospital management will store this information in the cloud server to enable the ECU people to take decision for patient's illness. To maintain the integrity of data's, in this work data is divided into multiple blocks and then each and every block will encrypted by using the unique cipher text class id. To support the scalability of data, dynamic creation of cipher text class id should be ensured for better decryption.

After deciding the number of cipher text class id's, the data blocks will be encrypted and then it will be stored in the cloud server. In this work, identity based encryption is used in which each and every patient data will encrypted by using the corresponding patient identity information and then the unique cipher text class id.

In this work, the number cipher text class ids generated are fixed at the dynamic time to support the scalability property. In the existing scenario, the number of cipher text classes to be generated will be decided by the tree level. But it is not sufficient to support the enormous amount of data generated in the run time. In this work elliptic curve concept is introduced which will decide the number of cipher text classes to be generated by using the specific classes of the elliptic curve. This elliptic curve method is based on the one time pad procedure. In this method, before deciding the number of cipher text classes, first the communication will be initialized between the user and the server. The user will send the amount of data needs to be transmitted and the server will send the number of cipher text classes need to have for processing the corresponding data. This will be decided based on the number of specific classes present in the elliptic curve.

STEPS:

1. Hospital management will encode the health care information and convert it into binary format

PT → encode (PT)
Message = encoded message

2. Encrypt the newly generated message using secret key

CT = Message ⨁Secret key

3. Send the cipher text to the KDC

Cloud server →send CT()

4. KDC will decrypt the message by taking XOR with the cipher text which is received

Message = CT ⨁Secret Key

In these steps, elliptic curve will be fixed as finite field where the point will made at each and every initialization of communication. Finally after completion of this communication, based on the length of the elliptic curve, the number of cipher text class id's will be decided. KDC will generate the number of cipher text class id's by using which encryption of data will made. After encryption, encrypted block of data will be stored in the cloud server.

B. Give the Access Permission in the Decentralized Environment**:** After encryption, the encrypted data blocks will be stored in the cloud server. Then in case of emergency situation ECU people need to be allowed to access the health care information that is stored in the cloud. However everyone is not allowed to gather the every details of the patient's health care information. To differentiate the access permission and support the multiple users who are located in different locations, in this work new role is introduced who is assumed as honest person.

Data will encrypted by using the access policy along with the identity information and the cipher text class id. The access policy is used to differentiate the access limitation of the ECU people. This access policy information will share with the KDC to provide the access permission key to the EU peoples. Trustee will generate one secret key and will keep aside with him.

In case of emergency situation, ECU people who receive the request from the patients will send access permission request to the trustee. The trustee will check the validity of users by checking their personal information and will distribute the secret key to ECI people. Then ECU people will take that key with them to the KDC. The KDC will match make the keys that are received from multiple users. If it matches together, then the secret key and the access policy will be given to the users.

STEPS:

1. ECU people will register them with trustee
2. Trustee will distribute the secret key to all registered users
3. Encrypt the data using ID, Cid, and Access Policy
4. Store it in the cloud
5. Send the access permission details to the KDC who are located in different location in the decentralized manner
6. ECU people requests access permission with the secret key given trustee
7. If (Key reside KDU = secret key given by trustee)
8. Provide them access permission
9. Else
10. Reply as invalid user
11. End if

C. Authenticate the Users before giving them Permission to Access the Contents: ECU people will retrieve the contents from the cloud server which are stored by the hospital management by using the keys that are distributed by KDC. Then proper prescriptions will made for the patients for their illness by analysing the health care information that are stored in the cloud and the symptoms sent by patients. To do so, first the authentication process will be initialized by submitting the secret information and access policy which are gathered from the users.

The cloud server will check whether the contents submitted by the ECU people are correct or not. If it is correct then the access policy is analysed and retrieve the health care information that are stored in the cloud to the ECU people with corresponding access permission.

D. Overall Flow of the System:

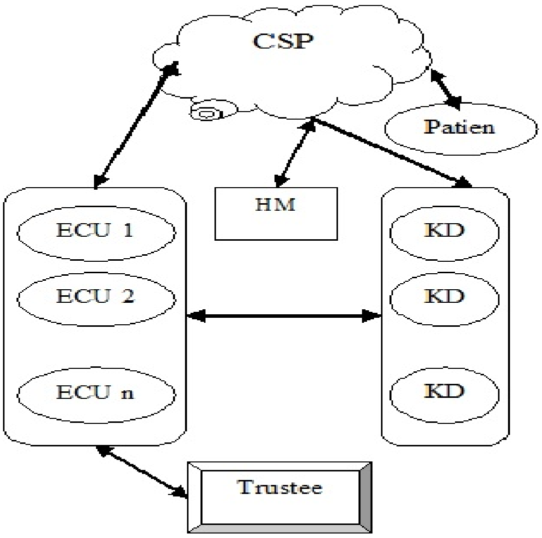

Figure 1. Flow Diagram

IV. EXPERIMENTAL RESULTS

The experimental results of our works proves that the proposed algorithm is efficient than the existing works. The performance evaluation of our work is done by comparing the proposed work with the existing algorithm based on some parameters which are listed as follows:

- Granted Keys
- Data Integrity
- Confidentiality

The parameter values which are obtained from the proposed approach decentralized privacy preserved health care monitoring service (DPHCM) with the existing approach called the key aggregate crypto system (KAC) are given in the following parameter comparison table.

Table 1. Parameter comparison Values

Parameter/technology	KAC	DPHCM
Granted Keys	3.0	3.5
Data Integrity	72%	82%
Confidentiality	78%	87%

A. Granted Keys:

The number of granted keys for decrypting the cipher text in both proposed approach and existing approach are compared in the below figure.

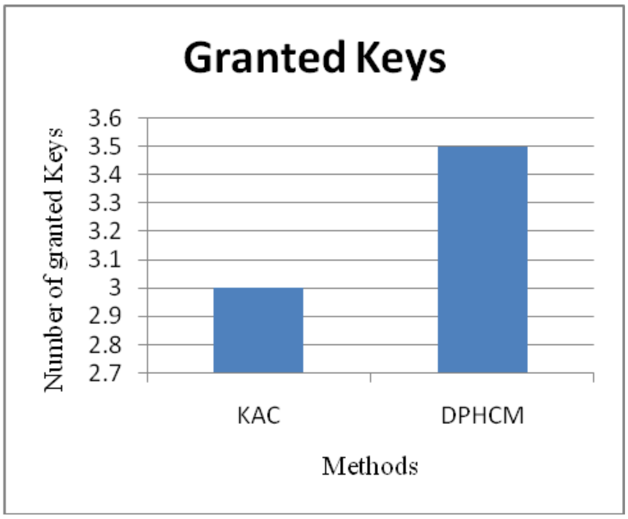

Figure 2. Granted Keys comparison

From the above graph it is proved that the proposed methodology provides better result than the existing approaches in terms of generating more number of cipher text class id's.

B. Data Integrity

Data integrity refers to maintaining and assuring the accuracy and consistency of data over its entire life-cycle, and is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data. ie., The accuracy and consistency of stored data, indicated by an absence of any alteration in data between two updates of a data record. The performance comparison of data integrity of existing methods with the proposed method are shown below.

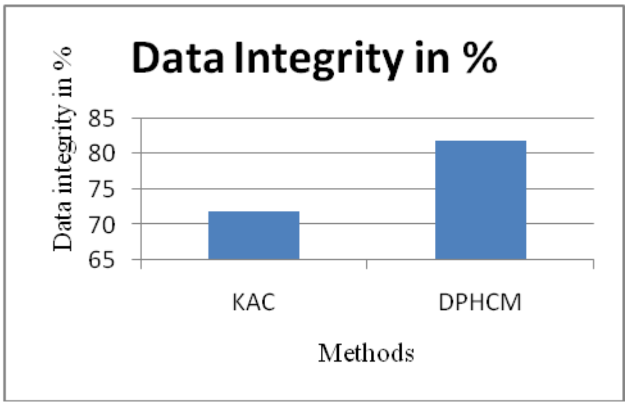

Figure 3. Data Integrity Comparison

From the above graph it is proved that the proposed methodology provides better result than the existing approaches in terms of data integrity.

E. Confidentiality:

Data Confidentiality is whether the information stored on a system is protected against unintended or unauthorized access. Since systems are sometimes used to manage sensitive information, Data Confidentiality is often a measure of the ability of the system to protect its data. Accordingly, this is an integral component of Security. The comparison measure of data confidentiality of our proposed work with the existing works is shown in below.

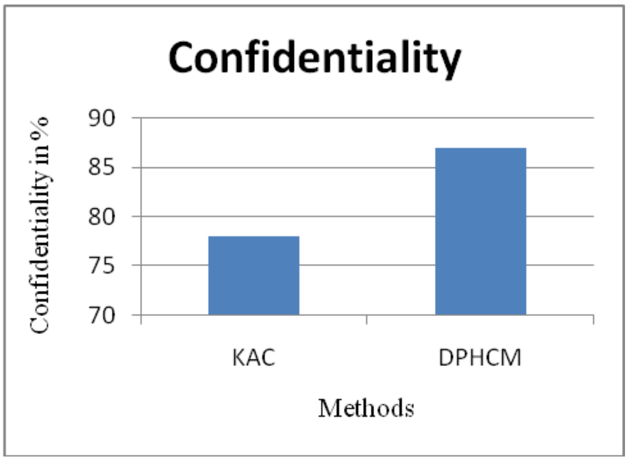

Figure 4. Confidentiality comparison

From the above graph it is proved that the proposed methodology provides better result than the existing approaches in terms of confidentiality.

V. CONCLUSION

Cloud monitoring plays a vital role in the real time environment which tends to provide a flexible environment for the cloud users through which they can get medical prescription. In this work, security risk is concentrated over the health care data's that are stored in the third party server called cloud service provider. The proposed work called decentralized privacy preserved health care monitoring service leads to better and flexible environment through which patients can store and access their data with promising guarantee of privacy. The experimental tests conducted were proves that the proposed methodology provides an better result than the existing approaches in terms improved system performance.

VI. REFERENCES

[1] Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014.

[2] Elaine Shi John Bethencourt T-H. Hubert Chan Dawn Song Adrian Perrig, "Multi-Dimensional Range Query over Encrypted Data", Proceedings of the 2007 IEEE Symposium on Security and Privacy, Pages 350-364, 2007.

[3] Huang Lin, Jun Shao, Chi Zhang, and Yuguang Fang,, "CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring", IEEE Transactions On Information Forensics And Security, Vol. 8, No. 6, June 2013.

[4] Sushmita Ruj, Milos Stojmenovic, Amiya Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", Cluster, Cloud and Grid Computing (CCGrid), 2012 12th IEEE/ACM International Symposium on 13-16 May 2012.

[5] Xavier Boyen , Brent Waters, "Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles)", Advances in Cryptology – CRYPTO, Volume 4117, pp 290-307 2006.