Multi-User Access Control and Key Management Mechanism for Personal Health Records

Thiruvenkatasamy S[1], Gopalakrishnan K[2]
[1]Assistant Professor, Department of Computer Science and Engineering,NandhaCollegeofTechnology, Erode, Tamil Nadu-638052, India, Email-samys.com@gmail.com.

[2]Assistant Professor, Department of Computer Science and Engineering,NandhaCollegeofTechnology, Erode, Tamil Nadu-638052, India, Email-gopalakrishnanbtech@gmail.com.

Abstract - Cloud computing technology helps individuals to store their essential information over the internet. The users can acquireinformationfromanywhere wheneverneeded. Duetothe advancesincomputertechnology,Cloud computing has gained an eminent deal of recognition among users. However the users should also be conscious of the privacy issuesof having information cached on the cloud. One ofthekeytoolstoassuresecurityforourdata is Cryptography. Therearenumerouscryptographic methods were available to promote security. Here in this paper, the AttributeBasedEncryptiontechniqueisemployedfor ensuring securitytoPHR (Personal Health Record). Personal health record represents a collection of health related information that has been created and maintained by the patient.

Keywords - Cloud Computing, Key Management, PersonalHealth Record, Attribute-Based Encryption.

I. INTRODUCTION

Cloud computinginpresentdays hasbecomeanemerging computing paradigm which helps out the users to cache thedata and retrieve the samewheneverneeded. It has a noble recognition among users [1]. The cloud computing technologyprovides numerous application services to comply with the user requirements. It introduces infrastructure-as-a- service (IaaS), platform-as-a-service (PaaS), or software-as-a- service (SaaS). The cloud environment permits the data owner to store their information and also to share the same with other users to whom they wish. Personal Health Record is one of the useful and great services furnished by the cloud technology. Personal health record is a stream of health related information that is created and maintainedby the patient. Now a day, personal Health Record (PHR) has turned out to be a patient- centric type of well-being health related information exchange. PHR comprises some information that can involve Personal Information like name, age, height, weight etc. It also includes prescription details, allergy facts and laboratory test details like blood test, X-ray images. There might also be a chance to hold some sensitive information like HIV profile, Cancer etc. The patient will have full control for their own medical records. They can share their health information with different users. The users can be from differentdomainswhich comprise healthcare providers, family members and friends. Security is the major thing in adopting cloud. This is because of the increase in the number of users in the present day. The data that has been cached in the cloud is getting increased every day and hence we are in need of some mechanisms in order to ensure that data that has been stored is in a secured manner. Issuing integrity for the data distributed over cloud is a challenging one.

In recent years, thecloud storage researchers have their centre of attention on the cryptographic process. That is to make sure that the data is not accessed by any unauthorized access in the network. Security for the information that has been saved in the cloud domain [2] is very important. Hence the chief answer to deal with this problematic situation is to use the cryptographic methods in cloud domain. Extensive Storage facility is one of the major advantages in cloud. To ensure security for the data stored in the cloud [3], cryptographic proficiencies can be embraced. The data or information has to get encrypted before the data owner actually uploads the data to the cloud in order to prevent the unofficial access to the sensitive data. This results in achieving security properties like authenticity, confidentiality,integrity,availability and reliability. In this paper, Attribute Based Encryption, a cryptographic approachisused to achieve security to PHR data in the cloud domain.

This article is structured as follows. Section 2 narrates about the Electronic health services in cloud domain. Section 3 and 4 reports securing the Health Record strategyand Literature survey. Section 5 describes about the existing system. Section 6showsproposed system architecture with moduledetails. Section 7 gives the conclusion about this article.

II. ELECTRONICHEALTHSERVICEINCLOUDDOMAIN

Electronic Health Service is one of thevery useful and life saving service. In 2009, Government of US announced a plan to pay out around19 billion dollars for computerizing the health (medical) records of the people to save life. In the

earlier days, the physicians maintain a medical report details in the paper.However nowadays, the advance in Information Technology has moved forward to an extent of caching the data to the cloud. The major advantage of doing so is,it is possible to access the medical record on the needed basis. The main goal of PHR is to furnish themedical health details regarding the patient. Personal Health Record is one of the key services issued by the cloud.It is a collection of health associated information which has been created and maintained by the owner i.e.) the patient. The data storage service is an important and useful service provided by the cloud provider [8].Given below are some of the benefits of caching Personal Health Records.

- Provides assistance to keep track of our health concerns like pressure level, cholesterol level, sugar level, etc.
- In case of emergency, it acts as a life saver as it helps to know the drug allergies of the patient.
- Insurance company may in need of PHR as they make payment for the patient in the Hospitals
- x-ray or other laboratory tests can also be examined and it also can be very useful in case of periodic checkups for thepatient.

As the numbersof users in using internet were getting increased in day to day life, a notable problem in using cloud domain is security. Basically achieving the security parameters like confidentiality, integrity and authenticity to the data that has been cached over cloud environment is a challenging one.Information that is cached in cloud with sensitive fields needs some protection [17]. To achieve this some approaches were required to check that our information is cached in a secured manner. Usage of some cryptographic methods in cloud environment can provide answer to this situation. This helps to assure security for the information that has been cached in the cloud environment.

III. SECURINGTHEHEALTHRECORDSTRATEGY

Theuserontheclouds houldbesurethatthedatathatthey havestorenotaccessedbyanythirdparty.Theuserscan employ somecryptographic methods to ensure security. Cryptography is a vitally important tool which helps to guarantee theaccuracyofthe information. Cryptographic approacheswereimplementedwidelyincloudenvironment fordatasecurity.ItgaveanimmensegrowthinthefieldofCloudComputingdomain.Cryptographicapproacheswere effectivelyleadbythegrowthofcloudcomputingandfurther also duetothebroadraiseintherange ofusersofthecloud.

The users of the Personal Health Record system can be care providers like doctors, dentists, Health insurers, pharmacist, nurses, Patient, his family members and friends. The personal domainofthePersonalHealth System includes patient's Family members and theclose friends of the patient. The public domain of Personal Health System includes Hospitals, Emergency department, Insurance Company etc. The data owner i.e., the patient may have some sensitive information like HIV, Cancer etc which they feel to hide. So in this case, the patient can use some encryption methods to protect the sensitive fields from unauthorized access.

The methods ofencryption provide security and privacy to the sensitive data. In the present days, the cloud storage researchers concentrate more on the cryptographic techniques. Thus the data confidentiality and authenticity can be attained on usingcryptographic approach in cloud computing environment. Patient Controlled Encryption [4] has been proposed by Josh Benolohatel, to secure the Electronic Medical Health Records that are stored in the cloud environment. KP-ABE (Key-Policy Attribute Based Encryption scheme) is employed by Shucheng Yu as a data encryption method to assure security. CP-ABE (Ciphertext Policy Attribute Based Encryption[5]isemployedbyLuanIbraimi asacryptographic technique to encrypt the data. MA-ABE (Multi- Authority Attribute Based Encryption) is also adopted to secure the PHR data [6]. This has been employed to improve security to Personal Health Record which has been viewed by the different departments.

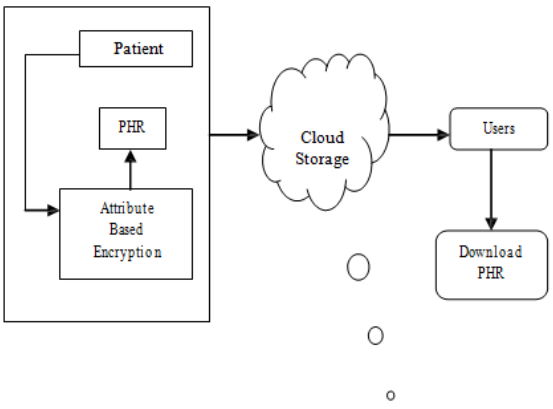

Fig 1: Cryptographic Cloud Storage Application

The cryptographic mechanisms were used to promote privacy to the data. The security properties like confidentiality, availability, integrity, authenticity, reliability can be assured. Thus a secured cloud storage environment can be achieved by the usage of the cryptographic methods.

IV. LITERATURE SURVEY

This part describes the works that are linked to the health record information that were cached in the cloud and different encryption approaches that were used to assure security for the data.

A model of E-Health system [13] is put in place by Ahmad et al. In the Electronic Health System, the health related information details are cached in the cloud domain. The information is created, saved and maintained by the health professionals such as Physicians, doctors, dentists, pharmacists etc. In the E-Health System, patients were not permitted to sight the medical detail that has been prepared by the physicians. However there may be some security problems gets perceivedinthisproposedsystem.Hencesome approaches were required to check and to ensure that the information is placed in a secured manner. Usage of Cryptographic methods in cloud environment helps to assure security.

Attribute-based Encryption is one of the cryptographic approaches that can be used in Cloud Computing domain. It is first launched by Sahai and Waters [10] in 2005. The chief basis of the ABE (Attribute-based Encryption) technique is to assure privacy to the information that has been cached in the cloud domain. In this scheme, data owner can use a set of attributes in order to encrypt the data to ensure privacy. The user who has the predicted attributes can decrypt the data. This encryption approach can fabricate the cloud domain more secure. KP-ABE is organized by Vipul Goyal and Omkant Pandey [12] toaccomplish fine-grained access control.In Key-Policy Attribute-based Encryption, the encrypted data is formed with the set of attributes which helps the authorized user to decrypt the text. In [14], Shucheng Yu et al employed Key-Policy Attribute-based Encryption. Bethencourt et al [9, 15] in the year 2007 advanced a approach called cipher text policy attribute-based method.In[5],Luan IbraimiappliedthiscryptographictechniqueCiphertextPolicy Attribute Based Encryption in order to encrypt the data. The owner of the data in this instance the patient is responsible for encrypting the sensitive information.

Melissa Chase and Sherman in [11], used Multi-Authority Attribute Based Encryption, a cryptographic approach to assure security. It comes in the group of advanced encryption approaches. This method can hold more number of users. Ming Li et al [7] gave a concept with two security domains, public domain and private domain. The public domain can have various departments and hence Multi-Authority Attribute Based Encryption has been used.

V. EXISTING SYSTEM

MingLietal[7]presentedthePersonalHealthRecordSystem withtwosecurity domains.OneisPersonaldomainandthe otherispublicdomain.Theformercomprisesfamilymembers andfriendswhereasthe lattercoversHospitals,Emergency section,InsuranceCompany etc.Thesedivisionsmainly handledtoovercomethe keycomplexityissues.The architectureforexistingsystemisgiven. To prevent unauthorizedaccesstoPHR,bothsecurity domainsuse AttributeBasedEncryption.Theownerof thedatais responsibleforselectingthe attributesandencryptingthe data. The encrypteddata isuploadedtothecloudenvironment. Clientscandecryptanddownloadthe PHR.Inthe existing architecture,theuseridentitybasedauthorization techniqueandthedistributedstoragemodel were notsupported. The architectureforanexistingsystemisshown.Inthearchitecture,PSD representsPersonalDomainandPUD representsPublicDomain.

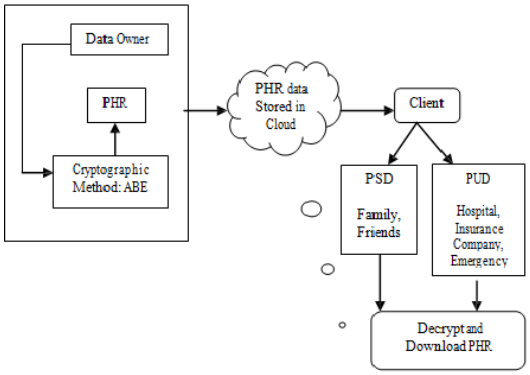

Fig 2: Existing System Architecture

VI. PROPOSED SYSTEM

In the proposed framework, Multi-Authority Attribute Based Encryption is enhanced to support PHR system with the distributed storage [16]. Multi-Authority Attribute Based Encryption is presented by Chase [6, 11] and it comprises of many authorities to govern the attributes and to handle the secret keys distribution function. The data owner select the sensitive attributes and he uses ABE approach to encrypt those sensitive attributes that he wish to hide for certain users. The five algorithms that are employed in this encryption operationare Set up, Attribute Key Generation, Central Key Generation, Encryption and Decryption. Once the PHR data is encrypted, the data owner has a responsibility to upload the same to the cloud domain.

ModuleDescriptions

Data Provider Registration

The first module is Data Provider Registration that permits the users to register themselves with the Data Provider. The data users can be of clients or Data owners. The registered user information can be viewed in the databases. The Data owner i.e. Patient will encrypt the data and transferthe same to the cloud providers.

Data Owner

Data owner plays a vital role in Personal Health Record system. He is responsible for selecting the sensitive attributes

Key Management

The key value for various authorities has been governed by this third module, Key Management. The data owner has a responsible to upload the key values. The key insertion and revocation responsibilities were covered in the Key management operation.

ABEOperation

ABE Operation module holds the Encryption process. The users who are authorized to viewthe PHR data can decrypt the data and download the data. In this paper, Attribute Based Encryption process is used for security purpose and to set up the distributed environment.

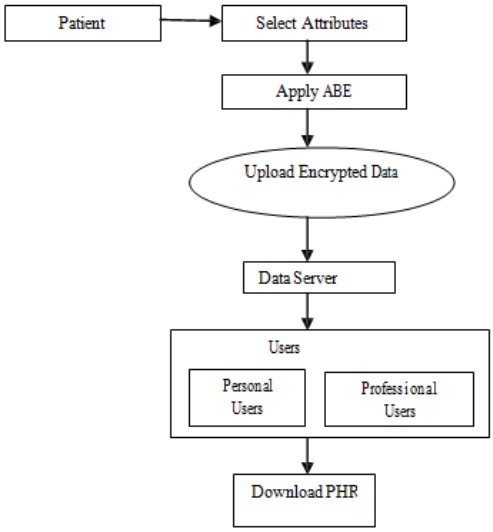

Fig 3 Data Flow diagram

AuthorityPerusal

The data owner is responsible for establishing the authority permissions. This module is planned to prove the users with their roles. The central authority is responsible for issuing the keys and the corresponding attributes.

User

The User module has been outlined for the users to access the PHR information whenever needed. As explained

earlier, the users can be of both personal and professional users who areauthorized to viewthe health record

VII. CONCLUSION

The key objective of our framework is to build a PHR system that lifts some functionality to the PHR data. The Health Related data can be cached and maintained by the Data owner in the data server of cloud environment. The proposed PHR system also comes up with excellent key revocation feature. In this article, the cryptographic technique ABE has been employed in order to promote security to the PHR data. The MA-ABE approach is intensified to hold up the distributed storage model of PHR system. Thus a secure sharing of PHR in a distributed environment has been accomplished in cloud computing Environment.

REFERENCES

P. Mell and T. Grance, "The nist definition of cloud computing", *NIST special publication.,* 800:145, 2011.

Patil D H&Bhavsar RR&Thorve A S, "Data security over cloud" *in IJCA Proceedings on Emerging Trends in Computer Science and Information Technology(ETCSIT2012).*,2012,ETCSIT (5):11-14

Bessani&Correia M&QuaresmaB,etal& DEPSKY,"Dependable and secure storage in a cloud-of-clouds", *6thConferenceon Computer Systems(EuroSys'11).,*2011:31-46

J. Benaloh& M. Chase& E. Horvitz&K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records",*Proc.ACM Workshop Cloud Computing Security (CCSW'09).,*pp.103-114,2009.

Ibraimi L, Tang Q&HartelP&JonkerW, "Efficientandprovable secure ciphertext-policyattribute-basedencryptionschemes", i*n: Bao,F.,Li,H.,Wang,G.(eds.) ISPEC2009.LNCS,vol. 5451, pages.1–12.Springer.*,Heidelberg(2009)

M. Chase,"Multi-authorityattributebasedencryption", in *TCC.,* pages515-534,2007

MingLi&ShuchengYu&YaoZheng&KuiRen&Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", *IEEE Transactions onParallelAndDistributedSystems.*,Volume24,No.1,January 2013.

Wu J & Ping L &GeXetal,"Cloud storage as the infrastructure of cloud computing", *inInternational Conference on Intelligent Computing and Cognitive Informatics.*,2010:380-383

Brent Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization",*in PublicKey Cryptography.,* pages53-70,2011.

V.S. Sureshkumar, Dr.M. Vijayakumar, "DDoS Attack Detection By using Traffic Flow Analysis for Streaming Data ", International Journal on Engineering technology and Science pp:2-7, Issue 8, volume 2,2015

A. Sahaiand and B. Waters,"Fuzzyidentity-based encryption," *inAdvancesinCryptology-Eurocrypt'05.*, pp.457-473, 2005.

ChaseMandChowS,"Improvingprivacyandsecurityinmulti- authority attribute-based encryption", *in Cloud Computing Security.*,pageno.121–130,2009.

Goyal O. Pandey & A. Sahai& B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," *in Proceedings of the 13'ACM conference on Computer and communications security.*, page. 89-98,2006.

H. Lohr& A.-R. Sadeghi& M. Winandy, "Securing the E- Health Cloud," *in Proceedings of the First ACM Int'l Health Informatics Symp. (IHI '10).*, pp. 20-229, 2010.

V.S. Sureshkumar ."Privacy *preservation for cloud Data using Triones in Multi cloud*", International journal of innovative Research in Engineering Science and Technology pp:1-7, Issue Special issue, volume3,2016

Shucheng Yu& Cong Wan&Kui Ren&Wenjing Lou,"Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", *in Proceedings of IEEE Communications Society for publication.*,2010, page. 534–542.

John Bethencourt& Amit Sahai&Brent Waters,"Ciphertext - Policy Attribute-Based Encryption",*in IEEE Symposium on Security and Privacy 07.*, pp. 321-334, IEEE, 2007.

V.S. Sureshkumar "Extended Framework For Dynamic Resource Allocation Using Asjs Algorithm In Cloud Computing Environment", International Journal on Engineering Technology and Sciences, pp:1-7, Issue 8, volume 1,2014

Muller& S Katzenbeisser&CEckert, "Distributed attribute based encryption",*in Proceedings of ICISC.*, pp. 20 -36, 2008.

Kamara S andLauter K, "Cryptographic cloud storage" *in 14th International Conference on Financial Cryptography and Data Security*., LNCS, IFCA/Springer Verlag. 2010, 6054: 136-149

Dhivyabala S andGopalakrishnan K, "Cloud Computing Model for Large Scale System through Merkle Hash Tree",*in International Journal of Innovative Research in Computer and Communication Engineering,* Vol.2, Special Issue 1,pp. 3856-3861, March 2014.

Nandagopal S&Karthik S&Arunachalam VP, "Mining of meteorological data using modified apriori algorithm",*in European Journal of Scientific Research*., Vol.47 No.2, PP.295-308, 2010.

Saveetha P and Arumugam S, "Study on Improvement in RSA Algorithm and itsImplementation", *in International Journal of Computer & Communication Technology*., Vol.3 No.6,PP.78, 2012.

Nithya K&KalaivaaniPCD&ThangarajanR, "An enhanced data mining model for text classification", *in International Conference on Computing, Communication and Applications.*,PP.1-4,2012.

VijayakumarM& Prakash S& ParvathiR.M.S, "Inter Cluster Distance Management Model with Optimal Centroid Estimation for K-Means Clustering Algorithm,"*in WSEAS Transactions on Communications*., Issue 6, Vol. 10, pp. 182-191, June 2011.

Vijayakumar M and Parvathi RMS, "Concept mining of high volume data streams in network traffic using hierarchical clustering",*inEuropean Journal of Scientific Research*., Vol.39,No.2, pp:234-242,January 2010.

Prakash S&Vijayakumar M & Parvathi RMS, "A novel method of mining association rule with multilevel concept hierarchy",*in International Journal Computer Application(IJCA.)*,PP:26-29,2011.

Nandagopal S&Arunachalam VP &Karthik, "A Novel Approach for Mining Inter-Transaction Item sets",*in European Scientific Journal*.,Vol.8,No:14,PP:92-108,2012.

Prakash S and Vijayakumar M, "An effective network traffic data control using improved Apriori rule mining", *in Circuits and Systems* 7,No: 10,3162-3173,August 2016.

Gokulraj P and Kiruthikadevi K, "Revocation and security based ownership deduplication of convergent key creating in cloud", *in International Journal of Innovative Research in Science, Engineering and technology.*, Vol. 3, Issue 10, ISSN: 2319-8753, October 2014.

Saveetha P&Arumugam S &Kiruthikadevi K, "Cryptography and the Optimization Heuristics Techniques", *in Int. Journal of Advanced Research in Computer Science and Software Engg.*, volume. 4, Issue.10, ISSN: 2277 128X, October 2014.

Vijayakumar M and Prakash.S, "An Improved Sensitive Association Rule Mining using Fuzzy Partition Algorithm", *in Asian Journal of Research in Social Sciences and Humanities.*,Vol.6,No.6,PP.969-981,2016.

Preethi B.C. and Vijayakumar M, " A Novel Cloud Integration Algorithm(CIA) for Energy Efficient High Performance Computing Applications in Big Data Multimedia Applications", *in Romanian Journal of Information Science and Technology.*, vol. 2, no.1, pp. 1-11, March 2018.