Efficient And Secure Privacy Preserving Data Storage and Auditability In Cloud Assisted Mobile Health Data

Sneha H. Rathi
Computer Science & Engineering
Rajiv Gandhi College of Engineering
Chandrapur, India
e-mail:snehur.rathi5@gmail.com

***Abstract*—** Today fast access to health data is very important .over that security of that data is important as well. With the increasing use of e-healthcare, large amount of health related data are present on cyber space. Thus it is very much essential to provide security to health data. As we know many of the insurance companies do not provide insurance and private company do not offer jobs the person with severe disease. Fast access of medical data improves quality of life and saves live in case of emergencies. Also remote monitoring reduces occupancy of hospitals and allows limited persons to be admitted

Over 8 million people are being suffered due to leakage of their health data. Thus we need some protocol , architecture, system to provide security and privacy to health data. outsourcing data storage and computation task has become more popular in cloud computing era .Our system offers salient features including efficient key management, privacy-preserving data storage, and retrieval, especially for retrieval at emergencies, and audit ability for misusing health data. Here We provide private cloud to each mobile user as a service to it. Public cloud acts as a service provider which offers private cloud to each user as a service. Mobile users outsource their data to private cloud and processed data is stored in public cloud this reduces computation task on mobile users

Keywords- *Access control; auditability; eHealth; privacy.*

*****

I. INTRODUCTION

With the deployments of mobile phones and smart phones monitoring of health data has become easy. Also less costlier way to store, monitor an access health data. With this cloud computing is latest technology being used in information technology. Cloud computing provide unprecended advantages in the field of IT on demand self survive ubiquitous network access location independent resource pooling ,usage based pricing .cloud assisted mobile health data is union of mobile health technology and cloud computing . With this it becomes easy access to health related data from any part of country. While these leads to exposure of data to outside world , thus privacy and preserving measure are demanded .thus out sourcing the data and computational task to the third party has become popular in world of computation .This reduces tremendous burden of computation and storage and security. Many companies use cloud computing technology .They use cloud to store and maintain the server reducing burden of an organization .Also they uses the experts to perform computational task more efficiently. We are provided with different cloud deployments models as was delivery models.

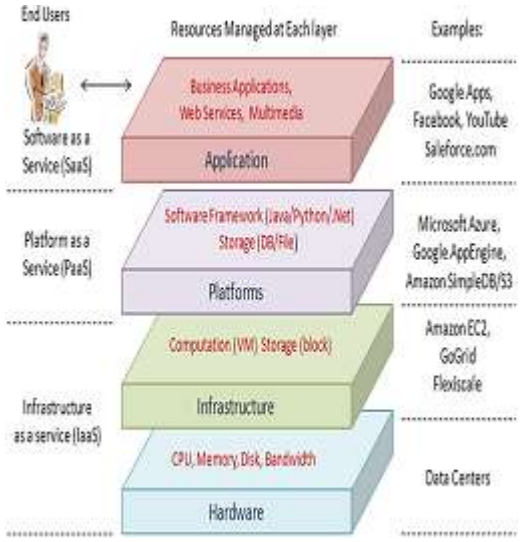
CLOUD DEPLOYMENT MODELS

- Public clouds: pubic cloud models are those that sells cloud to the required It provides resources to the web applications in need of it
- Private clouds: this cloud are given by public cloud. They are owned by the organisation and maintained controlled by the same
- Hybrid clouds: Its is the combine effect of both the clouds public cloud and private cloud .It posses property of both cloud .It is maintained by both the cloud.

DELIVERY MODELS:
There are three types of cloud delivery models

Software as a Service (SaaS):In this SaaS software act as a service to the user .like it act as service in web applications in the business, multimedia.
Platform as a Service (PaaS):it provide platform to the user so that different applications can found platform in the cloud eg googleApp.
Infrastructure as a Service (IaaS)It provides basic computation to the consumer as well as storage and resource computations It also look after storage and operating system .

In this project we use public cloud which provides private cloud to each mobile user .Private cloud perform computation and store the result into public cloud. We use different, more secure and reliable algorithm to provide privacy and auditing of the data stored to third party.



II. ISSUES IN CLOUD COMPUTING

There are many issues regarding security in cloud computing environment .This issues are to be removed from cloud environment as much as possible some of the issues reegardig cloud computing are explained as follows

1. Access Control

control is nothing but the degree with which user can have an access to the data Access can be read, write, modify .It is essential to allocate appropriate access write to different user With this authentication and authorities is combined to form refined access control

2. Attack/Harm Detection

This term indicates the amount of attack or attempts made to harm the system This attempts must be reduce as much as possible. As we use various transmission media to connect with cloud we have lots of threat in this transmission. Thus most of the attacks are made in http transmission

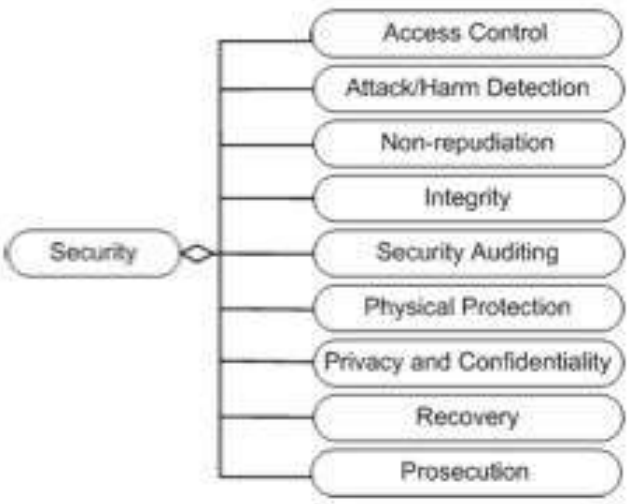


Figure 3 Security Issues in Cloud Computing

3. Non-Repudiation

It the amount with which two party communicate .it indicates repudiating factor that is denying of any aspect of making communication between users

As it offers mainly due to interactions, it can be controlled by having authorized transmission .This can be acquired by having public key transfer and authentication before transmission

4 Integrity

Integrity refers to the amount of change occur to the data. Integrity refers to data integrity, personal integrity and software integrity . Integrity can be maintained by printings from wrong access of data and maintaining confidentiality

5 Security Auditing

This term determines security related issues like auditing .here security personnel maintains audit, vulnerability of security mechanisms. Monitoring execution of the system and verifying and checking performs auditing well then traditional system

6 Physical Protection

It is nothing but physical damage to the system like damaging some part of the system .It also include stealing of some important part of the system. It Is nothing but the degree of protecting from physical attacks

7 Privacy and Confidentiality

Privacy and confidentiality is the degree with which data is safe from intruders so that they cannot understand it.It is the important task of most of the system we develop. To have strict confidentiality and privacy access control much be done More the access control greater will be the degree of privacy and security.

.

8 Recovery

Many a time we had data loss due to some hazards but if we have architectural features like hardware RAID, virtualizations the recovery of data is being made possible

9 Prosecutions

In case of cloud computing prosecution can be a legislative law to stop or to prosecute anything against law. Or it can be to prosecute the intruder or malicious user of data

.

III. LITERATURE REVIEW

1.P. Ray and J. Wimalasiri, "The need for technical solutions for maintaining the privacy of EHR," in Proc. IEEE 28th Annu. Int. Conf., New York City,NnY, USA, Sep. 2006, pp. 4686–4689.It explains the importance of medical data storage for the use .the solutions to it may be electronic

devices. They may include EPR (Electronic Patient record)HER (Electronic hHealth record).and EMR (Electronic medical Record)as this record is used by many health providers it is essential to provide privacy to the system .this paper provide security to important framework in Australia and HIPPA in America .

2. Charalampos Doukas,, Thomas Pliakas, Ilias Maglogiannis "Mobile Healthcare Information Management utilizing Cloud Computing and Android OS", 32nd Annual International Conference of the IEEE EMBS Buenos Aires, Argentina, August 31 - September 4, 2010 here cloud computing is used to support distributed environment .where data is stored in a cloud .Also bobile based application is developed to perform and maintail health record of the systemAmazons S3 cloud is used to provide service to the mobile userd

3. Nam Joon Park, Minkyu Lee, Dong-Soo Han, "A Mobile Healthcare Questionnaire Service Framework Using Composite Web Services" 978-1-4244-2281-4/08/$25.00_c 2008 IEEE Here questionnaire is used to determine the current condition of patient .web based application is being used and health questions and its analysis diagnose the problem to the person and provides remedies accordingly or model the interact with respect to medical conditions and contacts the other authority for it. also it looks for the near by place for the treatment of the problem.

4.Teh Amouh, Monica Gemo, Benoît Macq, Jean Vanderdonckt, Abdul Wahed El Gariani, Marc S. Reynaert, Lambert Stamatakis, and Frédéric Thys," Versatile Clinical Information System Design for Emergency Departments" IEEE Transactions On Information Technology In Biomedicine, Vol. 9, No. 2, June 2005 collaborative process of Emergency health care delivery is a complex process The real challenge is effective computerization of emergency department. Thus this computerization suffers various problems including inadequate data models, clumsy user interfaces, and poor integration with other clinical information systems To overcome this we consider three aspect first is transaction ,user interfaces and data management. Flexibility and adaptability is required for group task.

5. Arun George Eapen," Application of Data mining in Medical Applications" Waterloo, Ontario, Canada, 2004

Data mining is a relatively new field of research whose major objective is to acquire knowledge from large amounts of data. Due to availability of computers large amount of data is stored in computers .thus this data can be retrieved from computers .but to retrieve such large data and diagnose according to it is a difficult task. Thus data mining concept is used to obtain accurate decision in limited time. Also mobile computing is most fast way to access the data.Net can be used in Various devices to access the data by the user.

IV. SEQURITY REQUIREMENT

In this paper , we strive to meet the following main security requirements for practical privacy-preserving mobile healthcare systems The two main aims of our project is to obtain storage privacy and auditing

.

1) Storage Privacy:

Data stored on public cloud after computation should be provide privacy .this privacy include following 5 essentials

a) Data confidentiality:

data should be confidential tothe unauthorised user. Thus it should be unintelligent to the malicious user.

b) Anonymity:

No particular user is allowed to have an access to the medical data. Proper access right is given each user .the process is anonymous

c) Unlink ability:

Only authorised user is able to access the file .there should not be any unlink ability.That is no wrong link between user and data

d) Keyword privacy:

The keyword used for the data security should be kept confidential .because it may contain sensitive data . leakage of keyword can be very dangerous to the ultimate person

e) Search pattern privacy:

Search pattern used for the data retrieval should be kept private. Efficient SSE is required to solve this problem.Sstonger privacy preserving algorithm is required for Solving this problem

2) Auditability:

In emergency data access, the users may be physically unable to grant data access or without the perfect knowledge to decide if the data requester is a legitimate EMT. We require authorization to be fine-grained and authorized parties' access activities to leave a cryptographic evidence.

V. IMPLEMENTATION AND THREAT MODEL

1.Searchable Symmetric Encryption:

SSE is used to encrypt the data stored on the public cloud. It is also used for easy access to the data from the remote servers .SSE is used for the privacy of the data

KGen(s):This is used to generate a key used for the entire system. it take security parameter as input i.e s and gives the output as a key K used for encryption.

BIx (D,K):this function takes K as input and D i.e data file..It then output Index I .which contains index of all the data files can be used for retrieving data

TrapD (K ,w): It takes the Secret key K as input and w as input . To produce trapdoor tw . It act as a proxy for w. Tw should leak the information about w as little as possible.

SRCH (I, Tw): This function is executed by the remote server to search for documents containing the user defined keyword w. Due to the use of the trapdoor, the server is able to carry out the specific query without knowing the real keyword. The function takes the built secure index I and the trapdoor Tw , and outputs the identifiers of files which contains keyword w.

2. Attribute-Based Encryption:

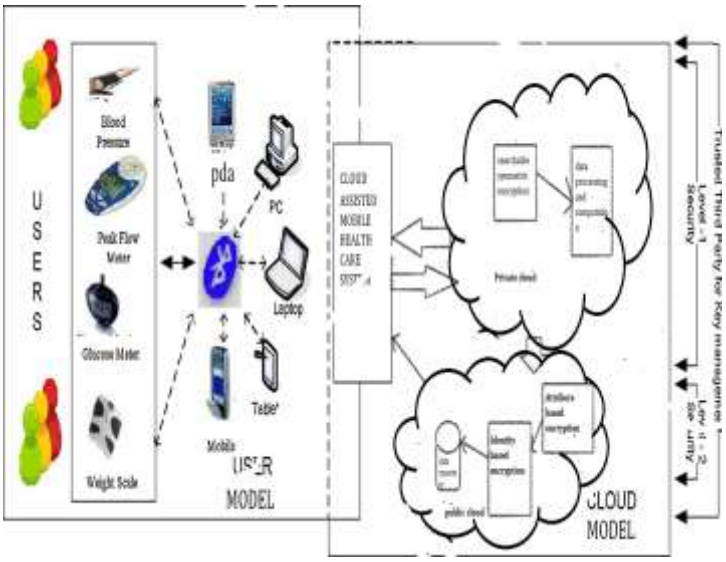
It is the refined over accessing of the out source data. Encrypt the data using the attributes use in the files .The attributes are used for decryption .If the attributes match with the data files the data is being accessed by the it

STUP: It takes only the security parameteas inputr.
It gives the public parameters PK and a master key MK.
KeyGen (MK,S**):** The key generation algorithm takes as input the master key MK and a set of attributes S that describe the key. It gives SK as output..
Encr (PK,A, M**):** It takes PK PK, a message M, and an access structure A over the universe of attribute as inputs. The algorithm will encrypt M and produce a cipher text CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message. Assume that the cipher text implicitly contains A.
Drypt(PK,CT,SK**):** it is used to decrypt the dat .it take public parameter PK as input and SK also cipher text CT .

Threat Model
Private cloud is the trusted cloud to perform data processing .public cloud is secure but has many intruder and not much secure. Thus require to be secured . Thus it is used to develop attributed based system EMT . Only the user having access right can access the data . Will maliciously drop users' packets, and access users . Thus the user do not having access right cannot have cess to the data

VI. ARCHITECHTURE

Here we see the architectural model of our project .our project consist of two main parts first is storage and computations and second is privacy and auditing
Here we are provided with cloud model consist of private and public cloud and user model user model obtain medical information from different sources like weight scale ,glucose meter and stores the result into mobile , laptop ,tablet, or anything like it .this data is computed in private cloud .thus reducing computing task on user .user is thus left with light weight processes. Also searchable symmetric algorithm is used to provide security to the storage data. This computed and encrypted data then goes to public cloud. Where it is stored in repository. Here we extract the attribute foe each file .also attribute based encryption and identity based encryption is used for encrypting data this helps for privacy of data as well as easy retrieval if data. Moreover it helps in auditing of the data. Here to levels of security is provided to the data in private and public cloud.



ACKNOWLEDGMENT

It is a pleasure to acknowledge the assistance of several people and institutions in this effort. Honestly speaking, this project has turned me into a debtor. First and foremost, I feel indebted to my guide, **Prof. Rahila Sheikh,** Assistant Professor, Department of Computer Technology, R.C.E.R.T, Chandrapur for her valuable guidance, continuous support and advice and constant encouragement throughout my project work. A special word of thanks goes to **Prof. P. S. Kulkarni**, Head, Department of Information Technology, R.C.E.R.T., Chandrapur and **Prof. R. K. Krishna**, Assistant Professor, Department of Electronics, R.C.E.R.T. for their encouragement to accomplish my work on time.

I am also grateful to **Prof. Nitin J. Janwe**, Head, Department of Computer Technology, R.C.E.R.T., Chandrapur for his last minute instructions which helped me to focus my work in the right directions.

I would like to extend my gratitude to honorable **Dr. K. R. Dixit**, Principal, R.C.E.R.T., Chandrapur, for being a constant source of inspiration.

Finally, I would like to extend my thanks to all those who have contributed, directly or indirectly to make this project successful.

REFERENCES

[1] Akhil Bhel, "Emerging Security Challenges in Cloud Computing", Information and Communication Technologies, 2011 World Congress on, Mumbai, 11th - 14th Dec 2011, pp 217 - 222, Print ISBN: 978-1-4673-0127-5, DOI: 10.1109/WICT.2011.6141247.

[2] Farzad Sabahi, "Cloud Computing Security Threats and Responses", IEEE 3rd International Conference on Communication software and Networks(ICCSN), 27-29 May 2011, pp 245-249, Print ISBN: 978-1-61284-485-5, DOI: 10.1109/ICCSN.2011.6014715.

[3] K.Mukherjee, G.Sahoo, "A Secure Cloud Computing", International Conference on Recent Trends in Information, Telecommunication and Computing, Mar 12th 2010, Washington DC

[4] Eman M.Mohamed, Hatem S Abdelkader, Sherif EI-Etriby, "Enhanced Data Security Model for Cloud Computing", 8th International Conference on Informatics and Systems(INFOS), Cairo, 14-16 May 2012, pp 12-17, Print ISBN: 978-1-4673-0828-1.

[5] Wentao Liu, "Research on Cloud Computing Security Problem and Strategy", 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 21-23 April 2012, pp 1216-1219, Print ISBN: 978-1-4577-1414-6, DOI: 10.1109/CECNet.2012. 6202020.

[6] Zhidong Shen, Qiang Tong " The Security of Cloud Computing System enabled by Trusted Computing Technology", 2nd International Conference on Signal Processing Systems, Dalian, (ICSPS), 5-7 July 2010, Vol 2, pp 11-15, Print ISBN: 978-1-4244-6892-8, DOI: 10.1109/ICSPS.2010.5555234.

[7] Aderemi A Atayero, Oluwaseyi Feyisetan, "Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption", Journal of Emerging Trends in Computing and Information Sciences, 1st Oct 2011, Volume 2, Issue 10, pp 546-552, ISSN: 2079-8407.

[8] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 9, pp. 1227–1239, Sep. 2010.

[9] J. Sun, X. Zhu, and Y. Fang, "Preserving privacy in emergency response based on wireless body sensor networks," in Proc. IEEE Global Telecommun.Conf., Dec. 2010, pp. 1–6.

[10] J. Sun, X. Zhu, and Y. Fang, "Privacy and emergency response in ehealthcare leveraging wireless body sensor networks," IEEE Wireless Commun., vol. 17, no. 1, pp. 66–73, Feb. 2010.

[11] J. Sun, X. Zhu, C. Zhang, andY. Fang, "HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare," in Proc. IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2011, pp. 373–382.

[12] L. Guo, C. Zhang, J. Sun, and Y. Fang, "PAAS: Privacy-preserving attribute-based authentication system for eHealth networks," in Proc. IEEE Intl. Conf. Distrib. Comput. Syst., Jun. 2012, pp. 224–233.

[13] J. Sun, X. Zhu, C. Zhang, and Y. Fang, Security and Privacy for Mobile Healthcare (m-Health) Systems, in Handbook on Securing Cyber-Physical Infrastructure, S. Das, K. Kant, and N. Zhang, Eds. Amsterdam, The Netherlands: Elsevier, 2011.

[14] E.-J. Goh, "Secure indexes," IACR Cryptology ePrint Archive, vol. 2003,p. 216, 2003.

[15] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," presented at the ACM Conf. Compute. Commun. Security, Alexandria, VA, USA, 2006.

[16] Y. C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. 3rd Int. Conf. Appl. Cryptogr. Netw. Security, 2005, pp. 442–455.

[17] D. Song, D.Wagner, and A. Perrig, "Practical techniques for searching on encrypted data," in Proc. IEEE Symp. Security Privacy, 2000, pp. 44–55.

[18] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious RAMs," J. ACM, vol. 43, pp. 431–473, 1996.

[19] R. Ostrovsky, "Efficient computation on oblivious RAMs," in Proc. ACM Symp. Theory Comput., 1990, pp. 514–523.

[20] C. Wang, K. Ren, S. Yu, and K. Urs, "Achieving usable and privacyassured similarity search over outsourced cloud data," in Proc. IEEE Conf. Comput. Commun., Mar. 2012, pp. 451–459.

[21] N. Cao, Z. Yang, C.Wang, K. Ren, andW. Lou, "Privacy-preserving query over encrypted graph-structured data in cloud computing," in Proc. IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2011, pp. 393–402.

[22] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable accesspolicy on PHI in ehealthcare systems," Adv. Health Inform. Conf., pp. 1–5, Apr. 2010.

[23] M. Katzarova and A. Simpson, "Delegation in a distributed healthcare context: A survey of current approaches," in Proc. 9th Int. Conf. Inform. Security, 2006, pp. 517–529.

[24] Foster, C.Kesselman,G. Tsudik, and S. Tuecke, "A security architecture for computational grids," in Proc. ACMConf. Comput. Commun. Security, San Francisco, CA, USA, 1998, pp. 83–92.

[25] X. Liang, R. Lu, L.Chen, X. Lin, andX. Shen, "PEC:Aprivacy-preserving emergency call scheme formable healthcare social networks" J. Commun. Netw., vol. 13, no. 2, pp. 102–112, 2011. L. Guo, C. Zhang, J. Sun, and Y. Fang, "A privacy-preserving attribute-based authentication system for mobile health networks," IEEE Trans. Mobile Comput., vol. PP, no. 99, pp. 1–1, 2013.

[26] W.-B. Lee and C.-D. Lee, "A cryptographic key management solution for HIPAA privacy/security regulations," IEEE Trans. Inf. Technol. Biomed., vol. 12, no. 1, pp. 34–41, Jan. 2008.

[27] C. C. Tan, H.Wang, S. Zhong, and Q. Li, "Body sensor network security: An identity-based cryptography approach," in Proc. ACM Conf. Wireless Netw. Security, Apr. 2008, pp. 148–153.

[28] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled Encr yption: Ensuring privacy of electronicmedical records," in Proc. ACM Workshop Cloud Comput. Security, 2009, pp. 103–114.

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

[30] C.-K. Chu, S. S. M. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Keyaggregate cryptosystem Trans. Parallel Distrib. Syst., vol. 99, no. PrePrints, p. 1, 2013. Available: http://doi.ieeecomputersociety.org/10.1109/TPDS.2013.112