Anonymous data exchange scheme in the public cloud and its application in the electronic medical record using Unified Modeling Language

Mannela Aswini [1] , A.Sandhya Rani[2]

1 PG Scholar, Dept. of CSE, Anantha Lakshmi Institute of Technology & sciences. Anantapuramu, Andhra Pradesh, India.

2 Associate Professor, Dept. of CSE, Anantha Lakshmi Institute of Technology & sciences., Anantapuramu, Andhra Pradesh, India

Abstract

Cloud computing is an on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centers available to many users over the Internet. Over the past few years, cloud computing has evolved quite quickly. Large amounts of data are uploaded and stored on remote public cloud servers, which users do not trust completely. In particular, most companies want to manage their data with the help of cloud servers. However, when outsourced data in the cloud is sensitive, the challenges of security and privacy are essential for the widespread deployment of cloud systems. This paper proposes a secure data sharing scheme to ensure the confidentiality of the data owner and the security of the outsourced cloud data. The proposed scheme provides a convenient advantage while addressing privacy and security challenges for data sharing. It demonstrates that the safety and efficiency analysis design scheme is feasible and effective. Finally, we discuss its application in the e-health (electronic health) record.

I. INTRODUCTION:

With the rapid development and application of cloud computing, more and more users are moving their data to cloud servers. The cloud computing technique alleviates the consumption of data management, data processing and capital expenditure for hardware, software and staff maintenance, etc. cloud server. The public cloud is owned and controlled by public cloud servers (PCS), which cannot be trusted. PCS could steal or obtain information on data stored by users. Therefore, many different security notions are proposed to ensure cloud security, such as remote data integrity, remote data exchange, etc. Data exchange is one of the important applications in cloud computing, especially for companies. Typically, a company can authorize certain entities to share their remote data based on the defined policy. However, data must meet the following security in most applications: 1)

data privacy information must be preserved; 2) unauthorized entities cannot obtain information from outsourced data and share your remote data with other users. Therefore, how to design a data sharing scheme while preserving the privacy and confidentiality of data in the public cloud is an urgent challenge. For example, it is normal for a user to have their own medical health data, including electronic health records, biomedical images, audio or video media, etc. This medical health data requires strict security protection as it involves patient privacy. To further study medicine and improve the standard of medical care, medical researchers must share patient data and extract valuable information. To find the general rule of data, these medical researchers will process a large amount of patient data directed at particular individuals. As medical / health data is private, patient identity information must be protected while their data is shared. At the same time, medical / health data can only be shared by authorized entities. Unauthorized subjects cannot obtain any information from medical / health data, i.e. the confidentiality of the data must be guaranteed. anonymity and confidentiality of data. With outsourced data, It is difficult to design an efficient way to share data while maintain the confidentiality of the identity of the data owners. To solve the previous problem, we investigated an anonymous data exchange scheme. Our contribution is twofold: First, let's give the formal model of achieving data exchange anonymity and confidentiality of data in public clouds. By analyzing the actual system and security requirements, we have provided the formal model and system security template. Second, we implement the data exchange scheme that it can obtain the protection of privacy and confidentiality of data in public clouds. Using symmetric encryption, searches can be performed attribute-based encryption and cryptography techniques; we design an efficient scheme that satisfies the security property.

II. DATA SHARING SCHEME:

The data exchange system model and its security model

are listed in this section. The data exchange scheme includes from three different entities, Cloud Server, Data owner and Data participant, as shown in Figure 1. They can be identified as follow:

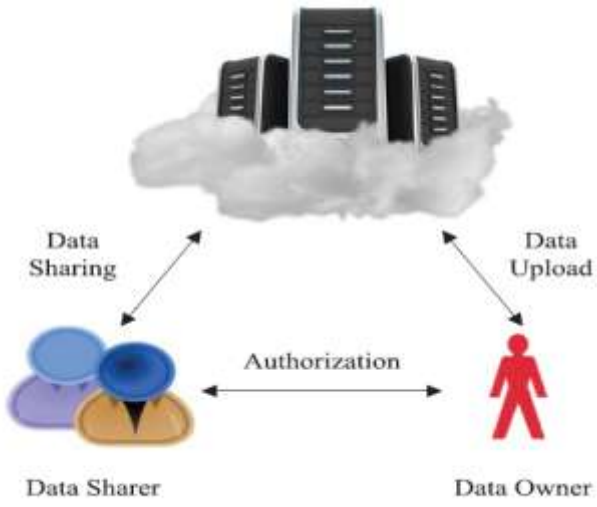


Fig1. The System Model of data sharing.

The cloud computing technique relieves consumer's data management, data processing and capital expenditure on hardware, software

and personnel maintenance, etc. Since data owners no longer own their data locally, it is important to ensure that the remote data is integer. When data owners authorize certain entities to share their data, it is important to share the authorized remote control efficiently data from those who share the data. In the proposed system we are using E-health, patient data are shared with different healthcare professionals. For E-health, many factors block the use of e-Health tools from widespread acceptance. Especially, patient records' privacy is the most important security issue. Most specifically, the E-health records need strong privacy preservation. This main concern has to handle the confidentiality of the data and the anonymity of the patient. The same security problems also exist when the E-health records are uploaded to the public clouds. By using the phases Sym-Enc, AB-Enc, S-Enc, Gen List of our scheme, the E-health records are encrypted and stored in the public clouds. When the authorized entity wants to access the remote E-health records which satisfy the specified conditions, it sends the corresponding challenge to PCS. By using the phase GenRetr, PCS sends the computed data V to the authorized entity. Upon receiving V, the authorized entity can retrieve the authorized data by using the phase retr of our scheme. Thus, by using our proposed scheme, E-health records can be securely shared in the public clouds.

III SYSTEM DESIGN

UML DIAGRAMS:

UML is asystematized acclaimed reason indicating language in the investigate item masterminded programming constructing. The terrific is overseen, and changed into made by using approach for using, the Object Management Group.

1. Give customers a readied to-use, expressive clean showing Language with the element that it will growth and interchange vital structures.

2. Give extendibility and specialization systems to improvement within character.

3. Be truthful of one in the whole part approximately sort programming tongues and headway approach.

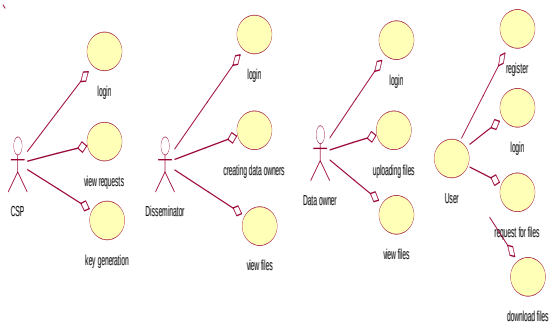
4. Give a trendy motivation to actual elements the showing language.

5. Connect with the improvement of OO hardware business assignment recognition.

6.Support better help motion worries which breakers made undertakings, frameworks, bureaucracy and bits. .

USE CASE DIAGRAM:

An utilization case Diagram inside the Unified Modeling Language (UML) is a sort of direct format portrayed thru and developed from a Use-case evaluation. Its idea is to show off a graphical examine the capacity gave thru a device to the volume on-display characters, their targets (addressed as use fashions), and any conditions a good sized lot of the ones use cases. The critical cause behind a use case graph is to find what gadget talents are practiced for which in undeniable view display individual. Employments of the performers in the framework are probably depicted.

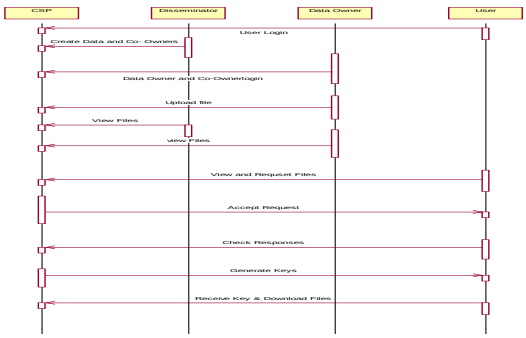


CLASS DIAGRAM:

In programming software organizing, a kind define Inside the Unified Modeling Language (UML) is a form of static shape graph that portrays the type of an equipment thru using contraption for displaying the shape's headings, their highlights, physical video games (or strategies), and the associations some of the mentoring.

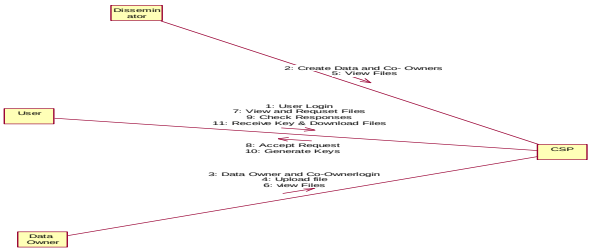
SEQUENCE DIAGRAM:

A recreation arrangement Diagram in Unified Modeling Language (UML) is a sort of participation diagram that endorses how approaches works of art with every actual and in what request. It is a skip on aggregately of a Message Sequence Chart. Social event lines are in fact and then forewarned as event diagrams, occasion situations, and timing charts.



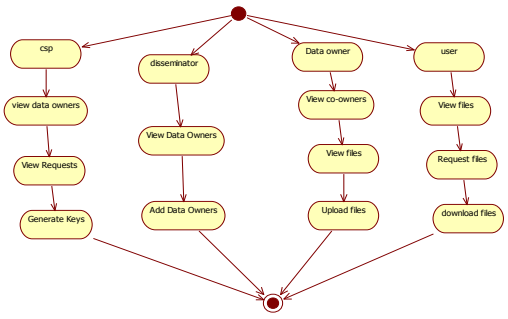
COLLABORATION DIAGRAM :

In composed exertion diagram the technique name game plan is exhibited via two or 3 numbering technique as dissected below. The showy introductions how the strategies are referred to as one after some other. We have taken the indistinct solicitation manipulate mechanical assembly to portray the joint exertion diagram. The technique calls are a number of equal to that of a sequence outline. Regardless, what's critical is that the range format does now not depict the thing association wherein in view of the reality the organized exertion graph suggests the affiliation.



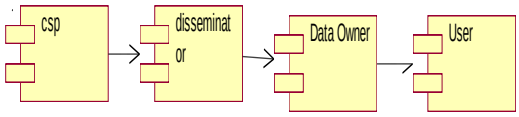
ACTIVITY DIAGRAM:

Activity plots are graphical depictions of work techniques of stepwise video games wearing sports sports andmoves with help for tendency, new dispatch and Simultaneousness. In the Unified Modeling Language, interest layouts may be used to explain the business and operational enhance by gadget for utilising step work techniques for portions in a device. An interest outline recommends the general float of manipulate



COMPONENT DIAGRAM:

Portion diagrams are carried out to provide a legitimization for the huge antique rarities of a system. This relic consolidates reviews, executables, libraries, and so forth. So the concept system in this diagram is considered as specific, Component graphs are applied over the span of the execution piece of an item. Be that as it could, it's far organized splendidly early to expect the usage bits of know-how. From the outset the tools is reliant the utilization of express UML plots and a short time later concurrently as the collectibles are prepared burden diagrams are used to get a idea of the execution.



DEPLOYMENTDIAGRAM

Organization graph speaks to the sending angle on a machine. It is identified with the issue outline. Since the segments are conveyed utilising the corporation charts. A sending define contains of hubs. Hubs are not some aspect however actual durable items used to established order the product application.

IV. SECURITY ANALYSIS AND PERFORMANCE ANALYSIS:

This section discusses the safety of our proposed scheme and performance. We give demonstrable security analysis**.**

The security of our proposed data sharing scheme is definite by the following security results.

Theorem 1: Denote the adversary as A. A interacts with the oracles of hash functions and the phase AB-E. The total number of the interaction can be bounded by the integer ^q. Then, in the AB-E security game, A's advantage is O (q^2/q). Theorem 2: Suppose the bilinear Diffie-Hellman (BDH) problem is complicated, our proposed data swap over scheme satisfies S-Enc security next to a chosen keyword assault in the random oracle model.

Theorem 3: According to the confidence in the PCS, our proposal. The data exchange scheme satisfies the anonymity of the data owner, that is, it is difficult to identify the real identity of the data owner for which you share data.

Information technology and communication are two important elements for the performance analysis of our schema. They are analyzed as

Computing - Before the data has been loaded, the data. The owner must perform the Sym-Enc, AB-Enc, and SEnc phases. Compared to AB-Enc and S-Enc, Sym-Enc is more efficient. In AB-Enc, the encryption algorithm will prompt

2 exponentiations in G1 for each sheet in the ciphertext access tree. For each leaf of the tree, the ciphertext size will include two elements of G1. The key generation algorithm requires exponentials for each attribute provided to the user and the private key consists of two group elements for each attribute. In S-Enc, to create the hatch for keyword, the data owner will perform a match and a boost. In Retr, the data sharer will cost you the calculation. The decryption algorithm requires two pairs for each

access the tree leaf and (at most) an upgrade for each node along a path from that leaf to the root. On the other hand, to send (A; B) to PCS, the data sharer will calculate one match and two exponentials. We execute our scheme and show its computation performance based on the up to date totaling technology.

Home page:

Data owner

Registration

Home page:

Profile:

Upload

View files:

View response

Public cloud:

Home page

Owners:

Owner files

View data sharer

Owner shared records:

View health records:

Data sharer

Register:

Home page:

Profile

Dataowner records

Response

Health record

Data upload

Response

V.APPLICATION IN E-HEALTH RECORD

By using E-health, patient data are shared with different healthcare professionals. For E-health, many factors block the use of e-Health tools from widespread acceptance. Especially, patient records' privacy is the most important security issue. Most specifically, the E-health records need more strong privacy preservation. This main concern has to handle the confidentiality of the data and the anonymity of the patient. The same security problems also exist when the E-health records are uploaded to the public clouds. By using the phases Sym-Enc, AB-Enc, S-Enc, GenList of our scheme, the E-health records are encrypted and stored in the public clouds. When the authorized entity wants to access the remote E-health records which satisfy the specified conditions, it sends the corresponding challenge to PCS. By using the phase GenRetr, PCS sends the computed data to the certified entity. Upon receiving V, the authorized entity can retrieve the authorized data by using the phase Retr of our scheme. Thus, by using our proposed scheme, E-health records can be securely shared in the public clouds.

VI. CONCLUSION:

In this, we proposed a data sharing scheme which can achieve the anonymity and data confidentiality in public clouds. We formalize the definition and the security model. Then, we designed a concrete data sharing scheme and gave the security proof. Security analysis showed our scheme is provably secure in the proposed security model. Performance analysis showed that our scheme is applicable.

REFERENCES

[1] C. Chu, S. Chow, W. Tzeng, J. Zhou, R. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp.468-477, Feb. 2014.

[2] Y. Tong, J. Sun, S. Chow, P. Li, "Cloud-assisted mobile-access of health data with privacy and auditability", IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 2, Mar. 2014.

[3] Z. Pervez, A. Khattak, S. Lee, Y. Lee, "SAPDS: Self-healing attributebased privacy aware data sharing in cloud", The Journal of Supercomputing, vol. 62, no. 1, pp. 431´lC460, Oct. 2012.

[4] C. Fan, V. Huang, H. Rung, "Arbitrary-state attribute-based encryption with dynamic membership", IEEE Transactions on Computers, vol. 63 no. 8, pp. 1951-1961, Apr. 2013.

[5] D. Boneh, G. Crescenzo, R. Ostrovskyy, G. Persianoz, "Public key encryption with keyword search", in Eurocrypt 2004, Interlaken, Switzerland May 2-6, 2004, pp.506-522.

[6] N. Cao, C. Wang, M. Li, K. Ren, W. Lou, "Privacy-preserving multikeywor ranked search over encrypted cloud data", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222-233, Nov. 2013.

[7] S. Seo, M. Nabeel, X. Ding, E. Bertino, "An efficient certificateless encryption for secure data sharing in public clouds", IEEE

Transactions on Knowledge and Data Engineering, vol. 26, no. 9, pp. 2107-2119, Sept. 2014.

[8] L.A. Dunning, R. Kresman, "Privacy preserving data sharing with anonymous ID assignment", IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp.402-413, Feb. 2013.

[9] X. Chen, X. Huang, J. Li, J. Ma, D. Wong, W. Lou, "New algorithms for secure outsourcing of large-scale systems of linear equations", IEEE Transactions on Information and Forensics Security, vol. 10, no. 1, pp. 69- 78, Jan. 2015.

[10] X. Chen, J. Li, J.Weng, J. Ma,W. Lou, "Verifiable computation over large database with incremental updates" IEEE Transactions on Computers, vol. 65, no. 10: 3184-3195, Oct. 2016.

[11] C. Gao, Q. Cheng, X. Li, S. Xia, "Cloud-assisted privacy-preserving profile-matching scheme under multiple keys in mobile social network", Cluster Computing, to be published. DOI: 10.1007/s10586-017-1649-y.

[12] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, Y. Tang, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks", Journal of Network and Computer Applications, vol. 106, no. 15, pp. 117-123, Mar. 2018.

[13] J. Li, X. Chen, X. Huang, S. Tang, Y. Xiang, M. Hassan, A. Alelaiwi," Secure distributed deduplication systems with improved reliability," IEEE Transactions on Computers, vol. 64, no. 12, pp. 3569-3579, Dec. 2015.

[14] J. Li, Y. Zhang, X. Chen, Y. Xiang, "Secure attribute-based data sharingfor resource-limited users in cloud computing", Computers & Security, vol. 72, pp. 1-12, Jan. 2018.

[15] J. Li, X. Huang, J.W. Li, X. Chen, X. Xiang, "Securely outsourcing attribute-based encryption with check ability", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 8, pp. 2201-2210, Aug. 2014.

[16] Y. Zhang, X. Chen, J. Li, D. Wong, H. Li, I. You, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing", Information Sciences, 379: 42-61, Feb. 2017.

[17] W. Sun, S. Yu, W. Lou, Y. T. Hou, H. Li, "Protecting your right: Attributebased keyword search with fine-grained owner-enforced search authorization in the cloud," in INFOCOM 2014, Toronto, Canada, Apr. 27-May 2 2014, pp.226-234.

[18] A. Rosenthal, P. Mork, M. Li, J. Stanford, D. Koester, P. Reynolds, "Cloud computing: a new business paradigm for biomedical information sharing", Journal of Biomedical Informatics, vol. 43, no. 2, pp. 342-353, Apr. 2010.

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

[20] J. Benaloh, M. Chase, E. Horvitz, K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records", in CCSW 2009, Chicago, Illinois, USA, Nov. 13, 2009, pp. 103-114.

[21] J. Sun, Y. Fang, "Cross-domain data sharing in distributed electronic health record systems", IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 6, pp.754-764, Jun. 2010.

[22] A. Bahga, V. Madisetti, "A cloud-based approach for interoperable electronic health records (EHRs)", IEEE Journal of Biomedical and Health Informatics, vol. 17, no. 5, pp.894-906, Sept. 2013.

[23] D. Anthony, A. Campbell, T. Candon, et al., "Securing information technology in healthcare", IEEE Security & Privacy, vol. 11, no. 6, pp. 25-33, Nov. 2013.

[24] M. Canim, M. Kantarcioglu, B. Malin, "Secure management of biomedical data with cryptographic hardware", IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 1, pp. 166-175, Jan. 2012.

[25] M. Lesk, "Electronic medical records: confidentiality, care, and epidemiology", IEEE Security & Privacy, vol. 11, no. 6, pp.19-24, Nov. 2013.

[26] S. Haas, S. Wohlgemuth, I. Echizen, N. Sonehara, G. Muller, "Aspects of privacy for electronic health records", International Journal of Medical Informatics, vol. 80, no. 2, pp.e26-e31, Oct. 2010.

[27] R. Zhang, L. Liu, "Security models and requirements for healthcare application clouds", in 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD), Miami, FL, USA, 2010, pp. 268-275.

[28] J. Fernandez-Aleman, I. Senor, P. Lozoya, A. Toval, "Security and privacy in electronic health records: a systematic literature review", Journal of Biomedical Informatics, vol. 46, no. 3, pp. 541-562, Jun. 2013.

[29] M. Ahmed, M. Ahamad, T. Jaiswal, "Augmenting security and accountability within the eHealth exchange", IBM Journal of Research and Development, vol. 58, no. 1, pp.8:1-8:11, Jan. 2014.

[30] F. Xhafa, J. Li, G. Zhao, J. Li, X. Chen, D. Wong, "Designing cloudbased electronic health record system with attribute-based encryption",