Data sharing in cloud computing

Himachal yadav

Student, Bachelor of Science (C.S.), Teerthanker Mahaveer University, Moradabad, U.P., India

himachalyadav6@gmail.com
namratakshp@gmail.com

Abstract-**Cloud computing is the development of parallel computing, distributed computing, grid computing and virtualization technologies which define the shape of a new era. Cloud computing is an emerging model of business computing. In this paper, we explore the concept of cloud architecture and compares cloud computing with grid computing. We also address the characteristics and applications of several popular cloud computing platforms. In this paper, we aim to pinpoint the challenges and issues of cloud computing. We identified sever challenges from the cloud computing adoption perspective and we also highlighted the cloud interoperability issue that deserves substantial further research and development. However, security and privacy issues present a strong barrier for users to adapt into cloud computing systems. In this paper, we investigate several cloud computing system providers about their concerns on security and privacy issues.**

Keywords **-** Cloud Computing, Access control, Personal Health Record, HASBE, Integrity, TPA, Homomorphic Linear Authenticator.

INTRODUCTION-

OVER CLOUD COMPUTING IS A GENERAL TERM FOR ANYTHING THAT INVOLVES DELIVERING HOSTED SERVICES OVER THE INTERNET. THREE IT IS SOLD ON DEMAND- GIVING THE CLOUD CONSUMER THE FREEDOM TO SELF-PROVISION THE IT RESOURCES, IT IS ELASTIC - WHICH MEANS THAT AT ANY GIVEN TIME A USER CAN HAVE AS MUCH OR AS LITTLE OF A SERVICE AS THEY WANT, THE SERVICE IS FULLY MANAGED BY THE PROVIDER-THE CONSUMER NEEDS NOTHING BUT A PERSONAL COMPUTER AND INTERNET ACCESS. OTHER IMPORTANT CHARACTERISTICS OF CLOUD ARE MEASURED USAGE AND RESILIENT COMPUTING. IN MEASURED USAGE CLOUD KEEP TRACK OF USAGE OF IT'S IT RESOURCES AND THE CONSUMER NEED TO PAY ONLY FOR WHAT THEY ACTUALLY USE. FOR RESILIENT COMPUTING, CLOUD DISTRIBUTES REDUNDANT IMPLEMENTATIONS OF IT RESOURCES ACROSS PHYSICAL LOCATIONS. IT RESOURCES CAN BE PRE-CONfiGURED SO THAT IF ONE BECOMES IMPERFECT, PROCESSING IS AUTOMATICALLY HANDED TO ANOTHER REDUNDANT IMPLEMENTATION.

RELATED WORKS -

This section reviews the concept of attribute based encryptions and provide a brief overview of Attribute Set Based Encryption(ASBE) and Hierarchical Attribute Set Based Encryption(HASBE).All these schemes are proposed as access control mechanisms to cloud To achieve scalability, flexibility and fine grained access control and efficient user revocation, Hierarchical attribute set based encryption [HASBE] by extending cipher-text-policy attribute set based encryption [CP-ASBE or ASBE] scheme is proposed. HASBE extends the ASBE algorithm with a hierarchical structure to improve scalability and flexibility while at the same time inherits the feature of fine-grained access control of ASBE. HASBE supports compound attributes due to flexible attribute set combinations as well as achieves efficient user revocation without requiring re-encryption because of attributes assigned multiple values.

PROBLEM STATEMENT -

Even though HASBE scheme achieves scalability, flexibility and fine grained access control, there is no

method called integrity scheme in HASBE to ensure that the data will be remained correctly in the cloud. Hence it is the major drawback of HASBE scheme. The data owners are facing a serious risk of corrupting or their data because of lack of physical control over their outsourced data. In order to overcome this security risk, privacy preserving public auditing concept could be proposed, which integrates data integrity proof with HASBE scheme.

OBJECTIVES -

The data owners want to prevent the server and unauthorized users from learning the contents of their sensitive file . Each of them owns a privacy policy. In particular, the proposed scheme has the following objectives:

Fine grained access control : Different users can be authorized to read different sets of files.

- User revocation:
  Whenever it is necessary, a user's access privileges should be revoked from future access in an efficient and easy way.
- lexible policy specification:
  The complex data access policies can be specified in a flexible manner.

Scalability:

To support a large and unpredictable number of users, the system should be highly scalable, in terms of complexity in key management, user management, and computation and storage.Enable users to ensure the integrity of data they are outsourced.

o Public audit ability:

to allow a Third Part Auditor (TPA) to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users. o Storage correctness: to ensure that there exists no cheating cloud server that can pass the TPA's audit without.

METHODOLOGY -

The entire system applies to Personal Health Record (PHR), which is an electronic record of an individual's health information. Online PHR service [8-9] allows an individual to create, store, manage and share his personal health data in a centralized way. Sincecloud computing provides infinite computing resources and elastic storage, PHR service providers shifthe data and applications in order to lower their operational cost.

The overall methodology of this work can be divided into two parts -

Secure PHR Sharing using HASBE and Secure data auditing. The architecture of Secure PHR sharing is given in figure 1 and secure data auditing .

Secure PHR Sharing -

For secure PHR sharing, HASBE has a hierarchical structure of system users. Hierarchy enables the system to handle increasing number of users without degrading the efficiency. PHR owners can upload their encrypted PHR files to cloud storage and data consumers can download and decrypt the required file from the cloud. In this system, the PHR owners need not be online all the time since they are not responsible for issuing decryption keys to data consumers. It is the responsibility of a domain authority to issue decryption keys to users under its domain. The system can be extended to any depth and in the same

level there can be more than one domain authorities so that no authority should become a bottleneck to handle large number of system users. Here the system under consideration uses a depth . hierarchy and there are five modules for secure PHR sharing-

1. Trusted Authority Module
2. Domain Authority Module
3. Data Ownenr Module
4. Data Consumer Module
5. PHR Cloud Service Module

1. Trusted Authority Module

- The trusted authority is the root or parent authority. It is responsible for generating and distributing system parameters and root master keys as well as authorizing the top-level domain authorities. In our system the Ministry of Health is the trusted authority.

Data Owner Module

- In our system patients are the data owners. A patient application is there which allows the patient to interact with PHR service provider. The main functions of these module are-

- Patients first register to the system and then log in.
- Patients can set the access privilege as who can view the files and upload encrypted files to cloud.
- Patient application performs encryption in two stages. First the file is encrypted with AES, then AES key is encrypted with patient specified policy and public key provided by NMA. Second stage corresponds to attribute set based encryption.

Data Consumer Module -

Medical professionals act as data consumers. Through the medical professional application doctors interact with PHR service provider.

- Each hospital administrator log in and creates employees by entering their details. Registration details are also given to NMA through web services.
- Doctors can later log in to the application using their username and password.
- The application allows doctors to view required patient details and download their files by interacting with PHR service provider in cloud through web services.

PHR Cloud Service Module-

Responsible for storing encrypted files. It preprocess the file for generating metadata for auditing purpose.

Secure Data Auditing -

Data auditing is performed by a third party Auditor (TPA) on behalf of the PHR service provider. For the cloud PHR service provideris the data owner. On the other hand PHR service provider is the client of TPA .verification details about uploaded files are given to TPA through proper communication channels. Upon getting data auditing delegation from PHR service provider, TPA interact with cloud and performs a privacy preserving public auditing. Homomorphic Linear Authenticator is used to allow TPA to perform integrity checking without retrieving the original data content. It issues challenges to cloud which indicates random file blocks to be checked. Cloud generates data correctness proof and TPA verifies it and indicates the result.

Related Work

- This section aims to present a summary of existing review articles related to secure data sharing in the Cloud. The review articles and surveys presented in this section donotfocusspecificallyonsecuredatasharinginth eCloud,ratherthemainrequirements that will enable it. The study of secure data sharing in the Cloud is fairly new and has become increasingly important with the advancements and growing popularity of the Cloud as well as the growing need to share data between people. There have been a number of reviews on security and privacy in the Cloud. Xiao and Xiao [14] identifies the five concerns of Cloud computing;confidentiality, integrity, availability, accountability, and privacy and thoroughly reviews the threats to each of the concerns as well as defense strategies. Chen and Zhao [15] outlines the requirements for achieving privacy and security in the Cloud and also briefly outlines the requirements for secure data sharing in the Cloud. Zhou [16] provided a survey on privacy and security in the Cloud focusing on how privacy laws should also take into consideration Cloud computing and what work can be done to prevent privacy and security breaches of one's personal data in the Cloud.

Privacy Issues

Privacy has many definitions in literature. Some examples of the different definitions of privacy are "being left alone", "the control we have over information about''.
ourselves" and also "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicatedtoothers"[26]tonameafew.TheOrganizationforEconomicCooperationand Development (OECD) [15] defines it as "any information relating to an identified or identifiable individual (data subject)". The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) in the Generally Accepted Privacy Principles (GAPP) standard [15] is "The rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information." From these definitions it is clear that a person has some level of control of what they want to disclose about themselves and want to keep the rest of their information kept secret. Privacy should not be assumed to have the same meaning as confidentiality. Confidentiality is allowing only authorised user's to gain access to that information and no-one else. We briefly explain the need of privacy and confidentiality in a number of fields.

Privacy and Confidentiality of data in Government:

Nearly all governments loans, earnings, medical costs, criminal offences and so on [31]. Governments also release data to the open public for its citizens to view. This may not guarantee the privacyofitscitizensassomeusermaybeabletoinferinformationaboutaparticular user through government data. In the United States for example, the Privacy Act of 1974 aims to protect an individual's privacy [32]. According to the Act, individuals have the right to see information the government has about but not limited to, unauthorized access of personal i[33] if information is leaked such as the controversy [34].

Privacy of data in Education:

Schools usually collect all students personal and health information. These include name, phone, address, contact details, details, medical history and family history to name a few.

Why Data Sharing is Important

Data sharing is becoming increasingly important for many users and sometimes a crucial requirement, especially for businesses and organisations aiming to gain profit. Historically, .However,inrecenttimes, it has been welcomed by a huge number of people as it has become significantly social [56]. It is thus not surprising that more and more people are demanding data sharing capability on their phones, computers and even recently Smart TVs. People love to share information with one another. Whether it is with friends, family, colleagues or the world, many people benefit greatly through sharing data.

Requirements of Data Sharing in the Cloud-

To enable data sharing in the Cloud, it is imperative that only authorised users are able to get access to data stored in the Cloud. We summarise the ideal requirements of data sharing in the Cloud .

• Any member of the group should gain access to the data anytime without the data owner's intervention.

• No other user, other than the data owner and the members of the group, should gain access to the data, including the Cloud Service Provider.

• The data owner should be able to revoke access to data for any member of the group.

• The data owner should be able to add members to the group.

• No member of the group should be allowed to revoke rights of other members of the group or join new users to the group.

• The data owner should be able to specify who has read/write permissions on the data owner's files. We now look at the privacy and security requirement of data sharing in the Cloud.

Traditional Approach-

. Zhao et al. [61], suggests a progressive elliptic curve encryption scheme (PECE) where a piece of data is encrypted a number of times using multiple keys and later decrypted using one key. Data sharing involves one user, say Alice, encrypting her data using her private key and storing the encrypted data to the Cloud. Another user, say Bob, sends a request for data access permission by sending his public key to Alice. Alice sends a credential to the storage provider for re-encryption of data and sendsacredentialtoBobtodecryptthedata.Thisisaneffectivetechniqueasitkeeps data confidential as data is encrypted through the entire stages thus never allowing a malicious user to view the plaintext data. This technique also does not allow the,inourcaseBob,ueis that it requires the data owner to be online at all times and hence makes it inefficient foreverydayusers.Thistechniquealsoassumestheprivatekeyoftheprovider is shared with the data owner. Realistically, no system administrator would want to share their keys with users and thus making it impractical to be deployed.

ABE for Data Sharing and Collaboration-

ABE is also used for data sharing and collaboration work al. made use of CP- and revocation. The department assigns users a set of attributes within their secret key and distributes the

secret key to the respective users. Any user that satisfies the access control policy defined by the data collaborator can access the data. When a user is revoked access rights, the data is re-encrypted in the Cloud rendering the revoked user's key useless. The scheme is proven to be semantically secure against chosen ciphertext attacks against the CP-ABE model. However, the scheme is not elegant in the case of user revocation since the updating of ciphertexts after user revocation places heavy computation overhead even if the burden is transferred to the Cloud.

CONCLUSION-

In this paper, we proposed the privacy preserving public auditing concept for HASBE scheme, to overcome the drawback of, absence of integrity assurance method in HASBE. Even though HASBE scheme achieves scalability, flexibility and fine- grained access control, it fails to prove data integrity in the cloud. Since, the data owner has no physical control over his outsourced data, such an auditing is necessary to prevent cloud service provider from hiding data loss or corruption information from the owner. Audit result from TPA would also be beneficial for the cloud service providers to improve their cloud based service platform, and users can give their data to the cloud and be worry free about the data integrity.The proposed system preserves all advantages of HASBE and also adds an additional quality of integrity proof to this system

REFERENCES:

[1] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, Senior Member, IEEE," HASBE: A Hierarchical Attribute set-Based Solution for Flexible and Scalable Access Control in Cloud Computing", ieee transactions on information forensics and security, vol. 7, no. 2, april 2012

[2] Kangchan Lee," Security Threats in Cloud Computing Environments", International Journal of Security and Its Applications ,Vol. 6, No. 4, October, 2012.

[3] Cheng-Chi Lee1, Pei-Shan Chung2, and Min-Shiang Hwang ,"A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments", International Journal of Network Security, Vol.15, No.4, PP.231-240, July 2013

[4] Vipul Goyal Omkant Pandeyy Amit Sahaiz Brent Waters," Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data"

[5] John Bethencourt, Amit Sahai, Brent Waters "Ciphertext-Policy Attribute-Based Encryption ", in Proc. IEEE Symp. Security and Privacy, Oakland, CA, 2007.

[6] Guojun Wanga, Qin Liu a,b, Jie Wub, Minyi Guo, Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers, www.elsevier.com locate / /cose

[7] Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran," Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption" University of Illinois at Urbana-Champaign, July 27, 2009

[8] Ming Li, Shucheng Yu, ,Yao Zheng, Kui Ren, and Wenjing Lou," Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption" in IEEE Transactions On Parallel And Distributed Systems ,2012

[9] Chunxia Leng1, Huiqun Yu, Jingming Wang, Jianhua Huang," Securing Personal Health Records in Clouds by Enforcing Sticky Policies" in TELKOMNIKA, Vol. 11, No. 4, April 2013, pp. 2200 ~ 2208 e-ISSN: 2087-278X.

[10] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou (2010), "Privacy Preserving Public Auditing for Data Storage Security in Cloud Computing".

[11] Jachak K. B., Korde S. K., Ghorpade P. P. and Gagare G. J.,"Homomorphic Authentication with Random MaskingTechnique Ensuring Privacy

& Security in CloudComputing", Bioinfo Security Informatics, vol. 2, no. 2,pp. 49-52, ISSN. 2249-9423, 12 April 2012

[12] Devi D," Scalable and Flexible Access Control with Secure Data Auditing in Cloud Computing", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4118-4123,ISSN:0975-9646