ISSN No. 0976-5697
Volume 6, No. 8, Nov-Dec 2015
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Efficiency of Security Privacy in Cloud Computing

M. R. Sudha
Assistant Professor
Department of Computer Science,
Faculty of Science and Humanities,
SRM University, Potheri, Kattankulathur – 603 203
Chennai, Tamil Nadu, India.

Abstract - Cloud services offer most services for the users to enjoy the on-demand cloud applications without considering the local infrastructure limitations. During the data accessing, different users may be in a collaborative relationship, and thus data sharing becomes significant to achieve productive benefits. The existing security solutions mainly focus on the authentication to realize that a user's privative data cannot be unauthorized accessed, but neglect a subtle privacy issue during a user challenging the cloud server to request other users for data sharing. The importance challenge access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions. In this paper, we propose a shared authority based privacy-preserving authentication protocol (SAPA) to address above privacy issue for cloud storage. In the SAPA, 1) shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations 2) attribute based access control is adopted to realize that the user can only access its own data fields; 3) proxy re-encryption is applied by the cloud server to provide data sharing among the multiple users. Meanwhile, universal Composability (UC) model is established to prove that the SAPA theoretically has the design correctness.

Keywords: cloud computing; privacy preserving; authentication protocol; shared authority

1. INTRODUCTION

Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications [1]. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth. Cloud computing is broken down into three segments: "application", "storage" and "connectivity." Each segment serves a different purpose and offers different products for businesses and individuals around the world [2, 11].Towards the cloud computing, typical service architecture is anything as a service (XaaS), in which infrastructures (IAAs), platform (PAAs), software (SAAs), and others are applied for wide spread interconnections[3, 12]

Moreover, it is not comfortable with the information that is stored in the cloud since security and privacy issues are becoming key concerns with the increasing popularity of cloud services. Conventional security approaches mainly focus on the strong authentication to realize that a user can remotely access its own data in on-demand mode [4, 13]. Along with the diversity of the application requirements, users may want to access and share each other's authorized data fields to achieve productive benefits, which brings new security and privacy challenges for the cloud storage [5, 14]. This form the basis of this research work to figure out the best way of sharing data in the cloud without exposing the authentication of the cloud users to unauthorized users [6, 15].

In the cloud environments, a reasonable security protocol should achieve the following requirements;

1) **Authentication:** a legal user can access its own data fields, only the authorized partial or entire data fields can be identified by the legal user, and any forged or tampered data fields cannot deceive the legal user.
2) **Data anonymity:** any irrelevant entity cannot recognize the exchanged data and communication state even if it intercepts the exchanged messages via an open channel.
3) **User privacy:** any irrelevant entity cannot know or guess a user's access desire, which represents a user's interest in another user's authorized data fields. If and only if the both users have mutual interests in each other's authorized data fields, the cloud server will inform the two users to realize the access permission sharing.
4) **Forward security:** any adversary cannot correlate two communication sessions to derive the prior interrogations according to the currently captured messages [16, 17].

2. OBJECTIVES OF SYSTEM AND SCOPE OF WORK

Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks towards the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure -coded data. The proposed design allows users to audit the cloud storage with very light weight communication and computation cost.

2. 1. Existing System

In the cloud storage based supply chain management, there are various interest groups (e.g., supplier, carrier, and retailer) in the system. Each group owns its users which are permitted to access the authorized data fields, and different users own relatively independent access authorities. It means that any two users from diverse groups should access different data fields of the same file. There into, a supplier purposely may want to access a carrier's data fields, but it is not sure whether the carrier will allow its access request. If the carrier refuses its request, the supplier's access desire will be revealed along with nothing obtained towards the desired data fields. Actually, the supplier may not send the access request or withdraw the unaccepted request in advance if it firmly knows that its request will be refused by the carrier. It is unreasonable to thoroughly disclose the supplier's private information without any privacy considerations.

DISADVANTAGES OF THE EXISTING SYSTEM

• Loss of data's.
• Does not provide any privacy for private data's.
• Authentication time takes too long.

2.2 PROPOSED SYSTEM

In this paper, we address the aforementioned privacy issue to propose a shared authority based privacy preserving authentication protocol (SAPA) for the cloud data storage, which realizes authentication and authorization without compromising a user's private information**.**

The main contributions are as follows.

1) Identify a new privacy challenge in cloud storage, and address a subtle privacy issue during a user challenging the cloud server for data sharing, in which the challenged request itself cannot reveal the user's privacy no matter whether or not it can obtain the access authority.
2) Propose an authentication protocol to enhance a user's access request related privacy, and the shared access authority is achieved by anonymous access request matching mechanism.
3) Apply cipher text-policy attribute based access control to realize that a user can reliably access its own data fields, and adopt the proxy re-encryption to provide temp authorized data sharing among multiple users.

ADVANTAGE OF THE PROPOSED SYSTEM

The scheme allows users to audit the cloud storage with lightweight communication overloads and computation cost, and the auditing result ensures strong cloud storage correctness and fast data error localization. During cloud data accessing, the user autonomously interacts with the cloud server without external interferences and is assigned with the full and independent authority on its own data fields.

3. LITERATURE REVIEW

In recent years, numerous research works on shared authority based privacy on how to preserved authentication in cloud environment have been carried out.

Cloud services as Internet-based IT services. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are three representative examples. As the cloud market becomes more open and competitive, Quality of Service (QoS) will be more important. However, cloud providers and cloud consumers have different and sometimes opposite preferences. If such a conflict occurs, a Service Level Agreement (SLA) cannot be established without negotiation [1]. They discussed much about Trust and security and how it has prevented businesses from fully accepting cloud platforms. To protect clouds, providers must first secure virtualized data center resources, uphold user privacy, and preserve data integrity. The authors suggest using a trust-overlay network over multiple data centres to implement a reputation system for establishing trust between service providers and data owners. Data colouring and software watermarking techniques protect shared data objects and massively distributed software modules. These techniques safeguard multi-way authentications, enable single sign-on in the cloud, and tighten access control for sensitive data in both public and private clouds [3]. A survey on the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations. The issue of Cloud storage and how it enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks towards the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure -coded data. The proposed design allows users to audit the cloud storage with very light weight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. Considering the cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Analysis shows the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks [2, 4]. Over the past few years, cloud computing has rapidly emerged as a widely accepted computing paradigm built around core concepts such as on-demand computing resources, elastic scaling, elimination of up-front capital and operational expenses, and establishing a pay-as-you-go business model for computing and information technology services. With the widespread adoption of virtualization, service oriented architectures, and utility computing there has been a significant development in the creation of cloud support structures to deliver IT services within QoS bounds, service level agreements, and security and privacy requirements. An architecture that differentiates security according to service-specific characteristics avoids an unnecessary drain on IT resources by protecting a variety of cloud computing services. In this paper, we address the construction of an efficient PDP scheme for distributed cloud storage to support the scalability of service and data migration, in which we consider the existence of multiple cloud service providers to cooperatively store and maintain the clients' data. We present a cooperative PDP (CPDP) scheme based on homomorphic verifiable response and hash index hierarchy. We prove the security of our scheme based on multi-prover zero-knowledge proof system, which can satisfy completeness, knowledge soundness, and zero-knowledge properties. In addition, we articulate performance optimization mechanisms for our scheme, and in particular present an efficient method for selecting optimal parameter values to minimize the computation costs of clients and storage service providers. Our experiments show that our solution introduces lower computation and communication overheads in comparison with non cooperative approaches [5-7].

Cloud computing will play a major role in the future Internet of Services, enabling on-demand provisioning of applications, platforms, and computing infrastructures. However, the cloud community must address several technology challenges to turn this vision into reality. Specific issues relate to deploying future infrastructure-as-a-service clouds and include efficiently managing such clouds to deliver scalable and elastic service platforms on demand, developing cloud aggregation architectures and technologies that let cloud providers collaborate and interoperate, and improving cloud infrastructures' security, reliability, and energy efficiency. Cloud computing rapidly expands as an alternative to conventional computing due to it can provide a flexible, dynamic and resilient infrastructure for both academic and business environments. In public cloud environment, the client moves its data to public cloud server (PCS) and cannot control its remote data. Thus, information security is an important problem in public cloud storage, such as data confidentiality, integrity, and availability. In some cases, the client has no ability to check its remote data possession, such as the client is in prison because of committing crime, on the ocean-going vessel, in the battlefield because of the war, and so on. It has to delegate the remote data possession checking task to some proxy. In this paper, we study proxy provable data possession (PPDP). In public clouds, PPDP is a matter of crucial importance when the client cannot perform the remote data possession checking. We study the PPDP system model, the security model, and the design method. Based on the bilinear pairing technique, we design an efficient PPDP protocol. Through security analysis and performance analysis, our protocol is provable secure and efficient [8, 10]

Digital Image and information embedding systems have a number of important multimedia applications. These systems embed one signal, sometime called an “embedded signal” or “information” within another signal, called as Host Signal [16].

In recent times, more and more awareness is paid to reversible data hiding (RDH) in encrypted images. Reason being, it maintains the superlative property that the original cover can be listlessly recovered after embedded data is extracted while shielding the image content’s privacy All earlier methods embed data by reversibly vacating room from the encrypted images. However, this may be subject to some slip-upon data extraction and/or image restoration. In this paper, we put forward a narrative method by reserving room before encryption with a conventional RDH algorithm. Hence, it is trouble-free for the data hider to reversibly embed data in the encrypted image. The projected technique can pull off real reversibility, that is, data extraction and image recovery are free of any error. We also develop a framework in which the performance of an information embedding method may be characterized based on its achievable rate-distortion-robustness trade-offs and discuss how previously proposed data hiding algorithms fit into this framework [9].

4. METHODOLOGY

We analyze the problem leakage on cloud computing security access during the authentication on private cloud. Each group owns its users which are permitted to access the authorized data fields, and different users own relatively independent access authorities. It means that any two users from diverse groups should access different data fields of the same file. There into, a supplier purposely may want to access a carrier’s data fields, but it is not sure whether the carrier will allow its access request. If the carrier refuses its request, the supplier’s access desire will be revealed along with nothing obtained towards the desired data fields. Actually, the supplier may not send the access request or withdraw the unaccepted request in advance if it firmly knows that its request will be refused by the carrier. It is unreasonable to thoroughly disclose the supplier’s private information without any privacy considerations.

We divided the research work into five modules ID GENERATION, USER CREATION, UPLOADING FILES TO SERVER, CLOUD SERVER, ALLOCATING RESOURCES TO USER.

4.1 ID GENERATION

In this module, we allocate Identity numbers to each and every user while registering into our group. In that we can collect information regarding the users present in the group as shown in Figure 1. We can also send and receive files from the user in our group or individual.

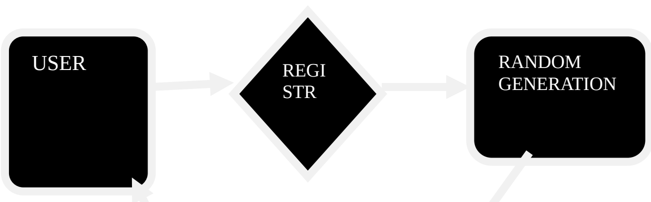

Figure1. ID Generation

USER CREATION

In this module, we have to create three kinds of users,

1. Supplier
2. Carrier
3. Retailer

4.2 UPLOADING FILES TO SERVER

In this module, we create a local Cloud and provide priced abundant storage services. The users can upload their data in the cloud as shown in Figure 2. We develop this module, where the cloud storage can be made secure. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to, we assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes, but will try to learn the content of the stored data and the identities of cloud users.

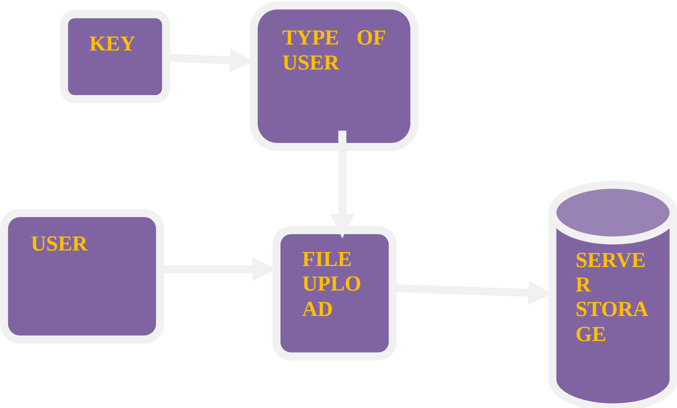

Figure 2. Uploading Files to Server

4.3 CLOUD SERVER

In this module, all the files we have uploaded by earlier modules are stored only with the help of cloud server represents the Figure 3. .

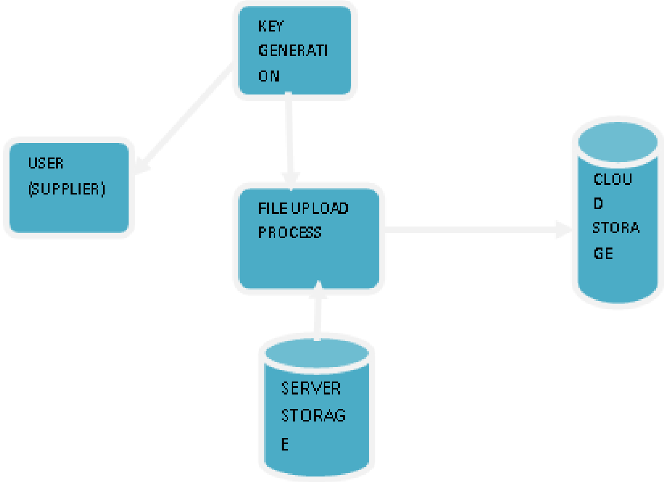

Figure 3. Cloud Server

4.4 ALLOCATING RESOURCES TO USER

In this module, the retailer needs to access files which have been uploaded by the supplier. If retailer wants to access file, first ask permission to the supplier who uploaded, then after he/she cannot send directly to the user which make a request. Then will go to carrier (acts as a third party) if carrier accepts the request made by user then only he/she can download

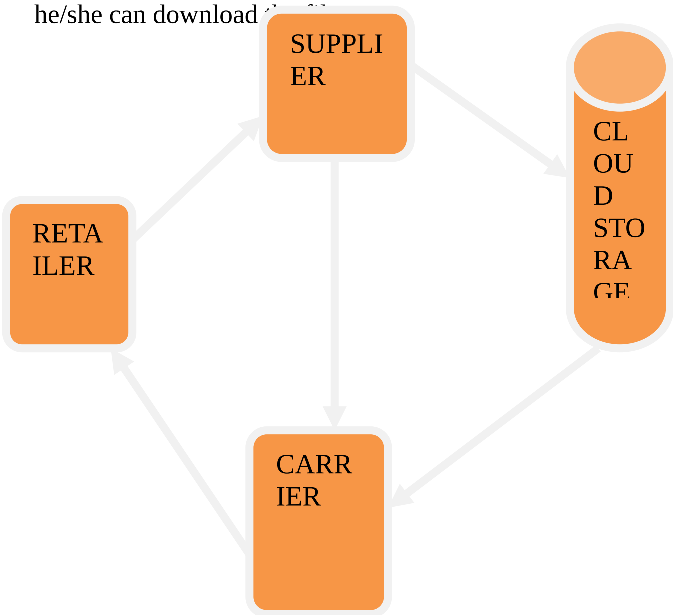

Figure 4. Allocating Resources to User

5. RESULTS AND DISCUSSION

Database design is the process of producing a detailed data model of a database. This logical data model contains all the needed logical and physical design choices and physical storage parameters needed to generate a design in a Data Definition Language (DDL), which can be used to create a database. A fully attributed data model contains details attributes for each entity.

5.1 SYSTEM DESIGN

SYSTEM ARCHITECTURE

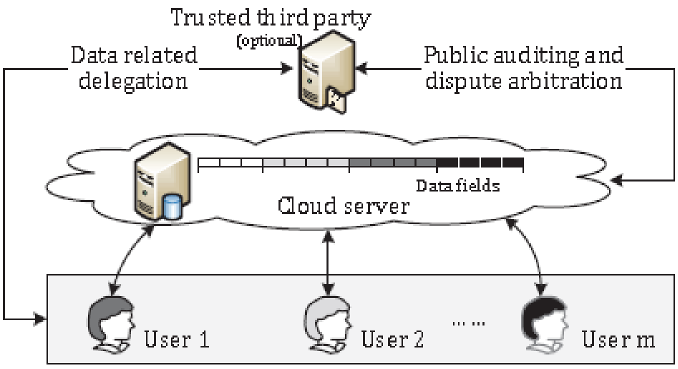

Figure 5. System Architecture

Figure.5. illustrates a system model for the cloud storage architecture, which includes three main network entities: users (Ux), a cloud server (S), and a trusted third party.

- **User:** an individual or group entity, which owns its data stored in the cloud for online data storage and computing. Different users may be affiliated with a common organization, and are assigned with independent authorities on certain data fields.

- **Cloud server:** an entity, which is managed by a particular cloud service provider or cloud application operator to provide data storage and computing services. The cloud server is regarded as an entity with unrestricted storage and computational resources.
- **Trusted third party:** an optional and neutral entity, which has advanced capabilities on behalf of the users, to perform data public auditing and dispute arbitration.

In the cloud storage, a user remotely stores its data via online infrastructures, platforms, or software for cloud services, which are operated in the distributed, parallel, and cooperative modes. During cloud data accessing, the user autonomously interacts with the cloud server without external interferences, and is assigned with the full and independent authority on its own data fields. It is necessary to guarantee that the users' outsourced data cannot be unauthorized accessed by other users, and is of critical importance to ensure the private information during the users' data access challenges. In some scenarios, there are multiple users in a system (e.g., supply chain management), and the users could have different affiliation attributes from different interest groups. One of the users may want to access other associate users' data fields to achieve bi-directional data sharing, but it cares about two aspects: whether the aimed user would like to share its datafields, and how it cannot expose its access request if the aimed user declines or ignores its challenge. In the paper, we pay more attention on the process of data access control and access authority sharing other than the specific file oriented cloud data transmission and management.

In the system model, assume that point-to-point communication channels between users and a cloud server are reliable with the protection of secure shell protocol (SSH). The related authentication handshakes are not highlighted in the following protocol presentation.

5.2 DATA FLOW DIAGRAM:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.

2. The data flow diagram (DFD) is one of the most important modelling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.

3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.

4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail as shown in Figure 6.

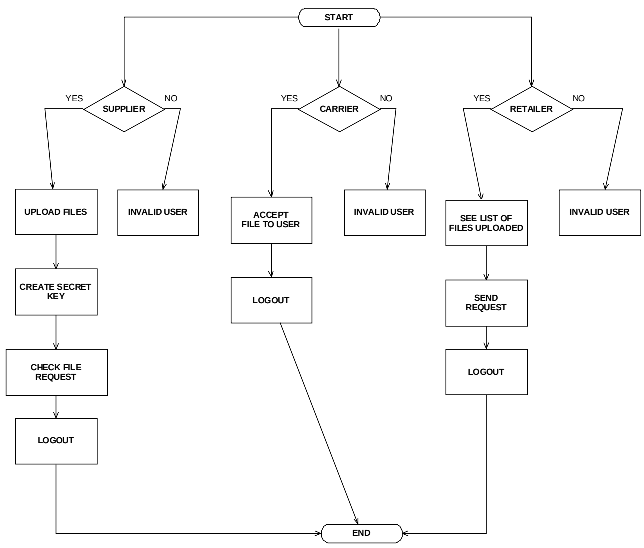

Figure 6. Data Flow Diagram

5.3 CLASS DIAGRAM

In software engineering, a class diagram in the Unified Modelling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.

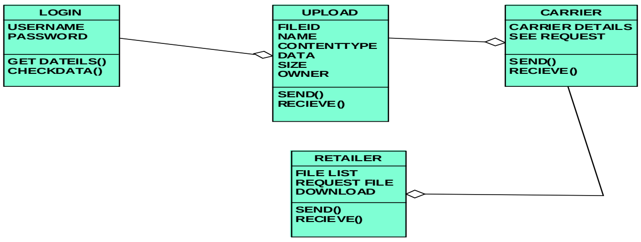

Figure 7. Class Diagram

5.4 ACTIVITY DIAGRAM

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modelling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. Figure 8 represents the activity diagram for the overall flow of control.

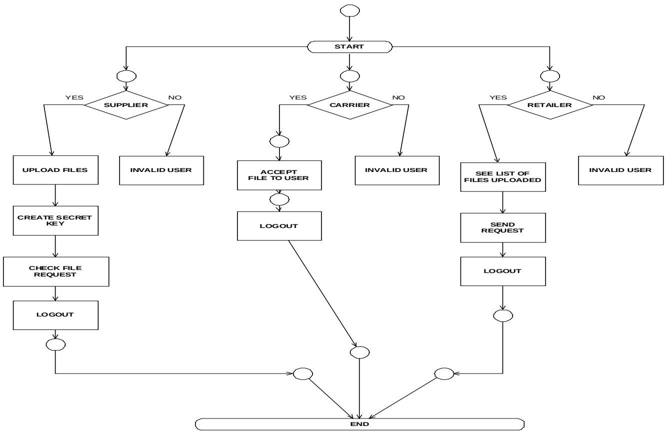

Figure 8. Activity Diagram

6. CONCLUSION

The shared authority based privacy protocol in the cloud is inspired by the power, flexibility, convenience and cost efficiency of the cloud-based data outsourcing paradigm. In this paper, we have identified a new privacy challenge during data accessing in the cloud computing to achieve privacy-preserving access authority sharing. Authentication is also established to guarantee data confidentiality and data integrity. Data anonymity is achieved since the wrapped values are exchanged during transmission. User privacy is enhanced by anonymous access requests to privately inform the cloud server about the users' access desires. It is hereby recommended that in the future the forward security should be use to realize the session identifiers to prevent the session correlation. This will indicate that the proposed scheme is possibly applied for enhanced privacy preservation in cloud applications. In future we can also use some other encryption and decryption techniques and compare it with existing system. By this comparison we can find the accuracy which one gives more privacy in cloud storage.

REFERENCES

[1] A.Mishra, R. Jain and A. Durresi, "Cloud Computing: Networking and Communication Challenges", IEEE Comm. Magazine, vol. 50, no. 9, pp.24 -25 2012.

[2] J. Chen , Y. Wang and X. Wang, "On-Demand Security Architecture for Cloud Computing", Computer, vol. 45, no. 7, pp.73 -78 2012.

[3] Y. Zhu , H. Hu , G. Ahn and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage", IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12, pp.2231 -2244 2012.

[4] H. Wang, "Proxy Provable Data Possession in Public Clouds", IEEE Trans. Services Computing, vol. 6, no. 4, pp.551 -559 2012.

[5] R. Moreno-Vozmediano, R.S. Montero and I.M. Llorente, "Key Challenges in Cloud Computing to Enable the Future Internet of Services", IEEE Internet Computing, vol. 17, no. 4, pp.18 -25 2013.

[6] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", IEEE Trans. Services Computing, vol. 5, no. 2, pp.220 -232 2012.

[7] K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Colouring", IEEE Internet Computing, vol. 14, no. 5, pp.14 -22 2010.

[8] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing", Natl Inst. of Standards and Technology, 2009.

[9] B. Tan, X. Shen and C. Zhai, "Qos Representation, Negotiation And Assurance in cloud Services" IEEE Internet Computing, vol. 14, pp.551 -559 2012.

[10] X. Shen, B. Tan and C. Zhai, "Secure Reversible Data Hiding In Encrypted Images by Allocating Memory Before Encryption VIA Security Keys" vol. 45, no. 7, pp.73 -78, 2013.

[11] S. Sundareswaran, A.C. Squicciarini and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud", IEEE Trans. Dependable and Secure Computing, vol. 9, no. 4, pp.556 -568 2012.

[12] Y. Tang , P.C. Lee , J.C.S. Lui and R. Perlman "Secure Overlay Cloud Storage with Access Control and Assured Deletion", IEEE Trans. Dependable and Secure Computing, vol. 9, no. 6, pp.903 -916 2012.

[13] Y. Zhu , H. Hu , G. Ahn , D. Huang and S. Wang, "Towards Temporal Access Control in Cloud Computing", Proc. IEEE INFOCOM, pp.2576 -2580 2012.

[14] S. Ruj, M. Stojmenovic and A. Nayak, "Decentralized Access Control with Anonymous Authentication for Securing Data in Clouds", IEEE Trans. Parallel and Distributed Systems, vol. 25, no. 2, pp.384 -394 2014.

[15] R. Snchez, F. Almenares, P. Arias, D. Daz-Snchez and A. Marn, "Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing", IEEE Trans. Consumer Electronics, vol. 58, no. 1, pp.95 -103 2012.

[16] H. Zhuo , S. Zhong and N. Yu, "A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability", IEEE Trans. Knowledge and Data Eng., vol. 23, no. 9, pp.1432 -1437 2011.

[17] Y. Xiao, C. Lin, Y. Jiang, X. Chu and F. Liu, "An Efficient Privacy-Preserving Publish-Subscribe Service Scheme for Cloud Computing", Proc. IEEE GLOBECOM 10, 2010.

