International Journal of Advanced Trends in Engineering and Technology (IJATET)
Impact Factor: 5.665, ISSN (Online): 2456 - 4664
(www.dvpublication.com) Volume 2, Issue 1, 2017

BI-LEVEL AUTHENTICATION FOR EFFECTIVE DATA SHARING IN CLOUD VIA PRIVACY-PRESERVING AUTHENTICATION PROTOCOL

J. Jeya Praise* & A. Sam Silva**
Assistant Professor, Department of Computer Science and Engineering, Rajas Engineering College, Tirunelveli, Tamilnadu

Cite This Article: J. Jeya Praise & A. Sam Silva, "Bi-Level Authentication for Effective Data Sharing in Cloud Via Privacy-Preserving Authentication Protocol", International Journal of Advanced Trends in Engineering and Technology, Page Number 23-30, Volume 2, Issue 1, 2017.

Abstract:
Cloud computing is an emerging technology of distributed computing where users can remotely store their data in cloud storage and enjoy the on-demand cloud applications and services from a shared pool of configurable computing resources, without the burden of local infrastructure and maintenance. During data accessing, different users may share their data to achieve productive benefits. Storing the data in third party's cloud system causes serious concern over the data confidentiality. The existing security approaches mainly focus on strong authentication to protect data from unauthorized accessed, but neglect a privacy issue when a user challenges the cloud server to request other user for data sharing. In this we propose a Privacy-Preserving Authentication (PPA) protocol for data sharing in cloud storage to address the above privacy issue. In the PPA, 1) Anonymous access request matching mechanism is used to achieve shared access authority with privacy and security consideration. (For e.g., user privacy, data anonymity, forward security and authentication); 2) Erasure code is applied by the cloud server to provide data sharing among the multiple users; 3) Attribute-based access control is applied to realize that the users can access only its own data fields. The bi-level authentication system is also proposed to authenticate the users in multiple levels using 2-level password generation technique which avoids the access of cloud servers from hackers.

Index Terms*:* Bi-Level Authentication, Cloud Computing, Data Sharing, Erasure code, Password Generation, Privacy-Preservation & Shared Access Authority

1. Introduction:

The term cloud computing is evolved from the cluster, grid and utility computing. Cloud computing provides high-throughput computing (HTC) paradigm. The infrastructure in cloud computing provides the services from a large data centre. The cloud computing allows the users to share access to resources from anywhere at any time through their connected devices. The cloud computing provides services such as: 1) Infrastructure-as-a-Service (IaaS), 2) Platform-as-a-Service (PaaS) and 3) Software-as-a-Service (SaaS) which are shown in Fig.1. These services allow the users to access services over the internet.

CLOUD SERVICES		
IaaS	SaaS	PaaS

Figure 1: Services offered by Cloud Computing

A cloud storage system focuses on designing a storage system for robustness, confidentiality, and functionality. A cloud storage system has many independent storage servers so that it is considered as a large-scale distributed storage system. In Cloud Computing, cloud data storage contains of two entities such as 1) cloud user and 2) cloud service provider/cloud server. The cloud user is a person who stores large quantity of data on cloud server which is managed by the cloud server. Without worrying about the storage and maintenance in cloud, the user can upload their data on cloud. The cloud server will provide services to the cloud user. To provide data robustness, one way is to replicate a message so that each storage server stores a copy of that message. This is very robust because the message can be retrieved as long as one storage server survives. Another way to provide data robustness is to use erasure coding. The erasure coding encodes a message of k symbols into a code-word of n symbols. To store the message, every code-word symbols is stored in different storage server. The security and privacy in Cloud Computing is a major issue with increasing number of cloud services. The security in Cloud Computing can be addressed in many ways as authentication, integrity and confidentiality. The existing security approaches mainly focuses on strong authentication to realize that users can remotely access their own data in on-demand mode. Along with this the users may want to access and share each other authorized data fields to achieve productive benefits. This brings a new challenge to security and privacy in cloud storage. The main contribution is to design a security scheme for data sharing in multiple user environments to simultaneously achieveaccess authority sharing, data access control and privacy. The privacy level of the data owner is raised and the confidentiality is increased. The privacy is accomplished by 2-level password generation and security in database is provided by erasure code, which will prevent the unauthorized data access from cloud. Researchers have worked to strengthen the protection of security and privacy preservation in cloud applications. There are various cryptographic algorithms for security and privacy problems, including security architecture [2], data public auditing protocols [3]-[5], secure data

storage and data sharing protocols [6]-[10], privacy preserving protocols [11] and key management [12]. However, most previous researches focuses on the authentication to realize that a legal user can access its authorized data only, which ignores the case that the different users may want to share and access each other's authorized data fields to achieve their productive benefits. When a user challenges the cloud server to access other users for data sharing, the access request itself may expose the user's privacy whether or not it can obtain the data access permissions. An effective privacy preserving authentication protocol (PPA) is proposed to enhance a user's access request related privacy and theanonymous access request matching mechanism is used to enhance shared access authority.The cipher text-policy attribute based access control is applied to realize that a user can reliably access its own data fields. The erasure code mechanism is applied for authorized data sharing during multiple users. The distributed storage system is used which depends on the secure cloud storage. The method used in PPA protocol is erasure code. By using the erasure code, the file which is uploaded by the owner which has been already encrypted will be splitted and zipped. The zipped file will be further stored in the database. The user can download the file by unzipping and merging the file stored from distributed cloud servers. The remainder of the paper is organized as follows: Section II introduces related works, Section III introduces the system model, Section IV presents the proposed authentication protocol, Section V presents the implementation and Section VI shows the experimental results and analysis of the proposed protocol. Finally, Section VII draws a conclusion.

2. Related Work:

Chen *et al*. [2] has proposed end-to-end security mechanism by dividing the larger security universe into three specific domains simplifies security policy delegation and makes it more practical. In cloud computing, the same provider might not offer network management, service provision, and storage. Thus, having three domains also fits well with different providers for these functions. Another advantage is simplicity. The user platform needs to configure only three inputs. Once the users order a service and specify the security level, the platform automatically factors in the service type and access network risk. Consequently, inputs are easy to manage and configure. It also makes it more practical to evolve traditional network systems to cloud computing. Because the security policy provides security on demand, there is no need to adapt security mechanisms for every domain. Consequently, architects can add security mechanisms in an existing network to our architecture without fundamentally changing them. Using existing network resources represents a substantial savings in efforts to deploy cloud computing. Kan*et al.* [3] proposed an efficient and secure dynamic auditing protocol, which protects the data privacy against the auditor by combining the cryptography method with the bi-linearity property of bilinear paring, rather than using the mask technique. The batch auditing protocol can also support the batch auditing for multiple owners. Furthermore, the auditing scheme incurs less communication cost and less computation cost of the auditor by moving the computing loads of auditing from the auditor to the server, which greatly improves the auditing performance and can be applied to large-scale cloud storage systems. Wang *et al.* [4] proposed a third-party auditor (TPA) that can do more efficient work and convince both cloud service providers and owners. The auditing is a natural choice for the storage auditing in cloud computing. The auditing protocol should have the following properties: 1) *Confidentiality:* The auditing protocol should keep owner's data confidential against the auditor. 2) *Dynamic auditing:* The auditing protocol should support the dynamic updates of the data in the cloud. 3) *Batch auditing:* The auditing protocol should also be able to support the batch auditing for multiple owners and multiple clouds. Recently, the author proposed several remote integrity checking protocols to allow the auditor to check the data integrity on the remote server. Lou *et al.* [5] proposed a dynamic auditing protocol that can support the dynamic operations of the data on the cloud servers, but this method may leak the data content to the auditor because it requires the server to send the linear combinations of data blocks to the auditor. The authors extended their dynamic auditing scheme to be privacy preserving and support the batch auditing for multiple owners. However, due to the large number of data tags, their auditing protocols may incur a heavy storage overhead on the server.

3. Problem Statements:

In the existing system a shared authority based privacy-preserving authentication protocol (SAPA) has been used to address the privacy issues on the cloud storage. The shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations. This protocol is used to address a user's sensitive access desire related privacy during data sharing in the cloud environments. The conventional security approaches mainly focus on strong authentication and does not consider about authorized data sharing in multiple user environment. The existing scheme does not have the option of granting or revoking data access.

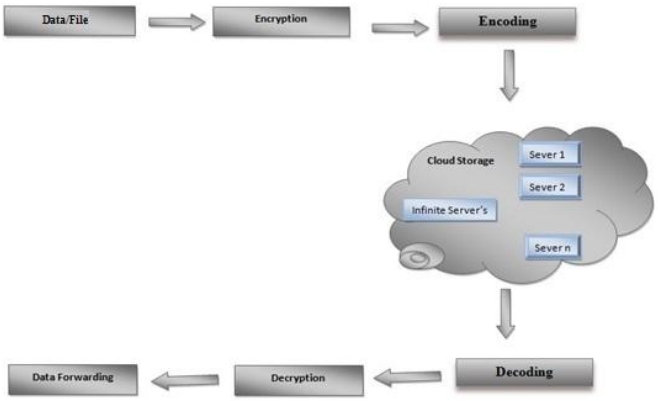

Figure 2: Existing System Architecture

4. Proposed Scheme:

An effective privacy preserving authentication protocol (PPA) is proposed to enhance a user's access request related privacy and the anonymous access request matching mechanism is used for sharingthe access authority. The cipher text-policy attribute based access control is applied to realize that a user can reliably access its own data fields. The erasure code mechanism is applied for authorized data sharing during multiple users. The distributed storage system is used which depends on the secure cloud storage. To verify whether someone is in fact authentication is an important process in any system. The authentication needs username and password,in any type of computer network such as private or public. To verify the person is authentic password is a secrete key. When a user wishes to use a system, the first thing is that the user has to register with the system, and thenaunique code is assigned for that person. On each consecutive use, the user must know the previously declared password for using it. The Bi-level authentication is a method which is proposed to restrict the un-authorized access of the users. The Bi-level authentication is proposed to generate and authenticate the 2-level password by considering the aspects of login credentials. This approach is used to decide whether the user can access the system or not. The Bi-level authentication mechanism provides security for the data contents of the cloud storage server by managing the identity and access control of the users. The access permission for users is provided by using 2-level password generation technique which can avoid unauthorized access of data from the cloud server and also provides security in login mechanism of user. By this the level of authentication is increased and the confidentiality of the data is raised by providing access to authorized users.It is secure and highly efficient for data accessing and data sharing in the multi-user cloud environment.

A. System Setup: The cloud storage system consist of a cloud server *S*, and users *{Ux}* ($x = \{1; :::; m\}$, $m \in \mathrm{N}*$). There into, *Ux* and *Uy*are two users, where they have independent access authorities on its own data fields. It refers that a user has access permission for particular data fields stored by *S*, and the user can't exceed its authority access to obtain other users' data fields. Now, consider *S* and *{Ux, Uy}* to present the protocol phases for data access control and access authority sharing with enhanced privacy considerations.

B. Proposed Protocol Description:

- ✓ **Access Challenges:** {Ux,Uy} respectively generates a new session identifiers {sidUx, sidUy}, then extract the identity tokens {TUx.Tuy} and it is transmited {sidUx||TUx, sidUy|| TUx} to S as an access query to initate a new session.
- ✓ **Access Control:** Ux first extracts it data attribute access list A_{Ux} to re-structure an access list L_{Ux}. Afterwards, *Ux* randomly chooses $\beta \in Zq$, and the decryption key *kAUx* for *AUx*can be obtained. Afterwards, Ux computes a setof values to establish a ciphertextCUx.
- ✓ **Request Matching and Data Sharing:** Upon receiving the ciphertexts*{CUx ,CUy}* within an allowable time interval, and *S* extracts *{PIDUx, PIDUy}* to derive the access requests *{RUyUx,RUxUy}*. *S* checks whether *{RUyUx,RUxUy}* satisfy $F(RUyUx(RUxUy)T) = F(2) = Cont$. If it holds, *S* will learn that both *Ux* and *Uy* have the access desires to share its authorized data fields with each other, and to access each other's authorized data.

C. System Architecture: The overall system architecture is given in Fig 3 where the data provider, secure cloud storage and data consumer form data access authority sharing. The process starts with the data owner, cloud storage followed by the receiver. Finally the overall performance of the system is analyzed.

The system architecture for the cloud storage includes two main network entities

- ✓ Users (Ux)
- ✓ Cloud Server (S)

The user (Ux) is an individual or group entity, which owns its data stored in the cloud data storage and computing. In a common organization, different users may be affiliated with certain data fields which are assigned with independent authorities. A user can be a data provider and a data consumer simultaneously. The

cloud server (S) is an entity, which is managed by a particular cloud application operator to provide data storage and computing services or a cloud service provider. The cloud server is regarded as an entity with unrestricted storage and computational resources.

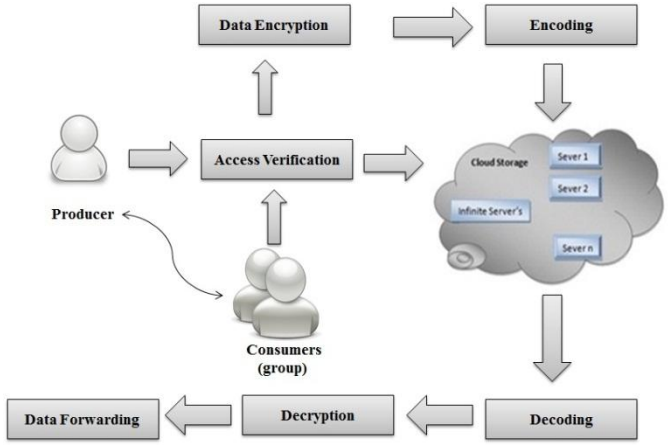

Figure 3: Overall System Architecture

In the process, at first the data owner encrypts the message (files) and splits the message into number of files and outsources the splitted files to the distributed server by zipping the files. The server validates the outsourced cipher texts and stores them for the owner.The permission for accessing the data is provided by the provider on receiving the request from the consumer thus it is more secured while transferring the files. During cloud data accessing, the user autonomously co-operates with the cloud server without external interferences and with full and independent authority on its own data fields is assigned. It is essential to guarantee that the users stored data cannot be unauthorized accessed by other users.It is a critical challenge to ensure the private information during the users' data access challenges. For that, the access verification is performed by the Bi-level Authentication mechanism which generates two passwords in two levels using the two-level password generation technique. Every level requires an authentication details. Based on that authenticated password, consumers can access the data stored in the cloud. Before generating password, user has to face the user interface protocol to enter the details.Based upon the user interface inputs, password generates automatically and retains generated password to access the cloud data.The server stores a single file in distributed virtual machines so an attacker who tries to misuse the file will fail to view or access the whole content due to the splitting of files and storage in different cloud environment. Finally, during the retrieval of file, the files in different storage systems are merged and the whole content is decrypted and then it can be downloaded from the server by performing the verification process for the user or retriever credentials. The server will provide a secret key for every user who accesses the data.

5. Implementation:

Sharing a file has never been easier with cloud storage. Most cloud storage services provide file sharing features which can allow sharing a file or folder with ease but not for multi user environment.A security scheme is proposed to simultaneously achieve data access control, access authority sharing and privacy. The process has been divided into six phases.

Process Initialization: The process of the security scheme begins with the data provider. An owner who has to upload their files in a cloud server, he/she should register first. For that he/she needs to fill the details in the registration form. These details are maintained in a database.To upload a file in cloud then the provider has to get login access. The type of file accepted for upload by this application is data files and image files and there is no limitation of the size of the file, which provides flexibility to the user. The person with valid credentials has the access rights to perform login for that they should login by giving their login credentials which has been registered in the database at the time of their registration.The data consumers are the users who want access the shared data stored in the cloud. If a user wants to access the shared data which is stored in a cloud, then he/she should register their details first. These details are maintained in a Database. If the user is an authorized user, he/she can download the file by using file id which has been stored by data owner when it was uploading.

Access Verification: The verification process of the data provider is performed by the login credentials. Password is a secrete key to verify that the provider is authentic. The verification process of the data consumer is performed by the Bi-level authentication mechanism. The Bi-level authentication mechanism is proposed to generate and authenticate the two-level password by considering the login credentials for the consumers to avoid access form the un-authorized users. The first level password generation is a user level password. The user level password generation will verify the requested consumers are authorized users. It authenticates the user privileges. The consumers need to enter user name, date of birth, employee id and group name to generate his/her password. The algorithm will process these inputs and generate the privilege authentication password. The privilege password helps move into the intra group. The second level password generation is a group level

password generation to authenticate the group for the particular service. The consumer needs to enter the privilege password to get the group level password. The group password will be generated while the entered password is match in the database. After the verification is over the consumer will be provided with a group password. The group password helps the consumer to access the cloud data for that particular user.

File Transfer: The file transfer is the act of copying or transferring the file from providers' devices to cloud storage. In this process, the encryption is done. Encrypting files is a way to protect the data from unwanted access. The data can be encrypted by using AES encryption mechanism. The AES algorithm operates on bytes, which makes it simpler to implement and explain. The key length can be 16, 24 or 32 bytes. This key is expanded into individual sub keys, a sub keys for each operation round. This process is called key expansion. Since AES is an iterated block cipher the same operations are performed many times on a fixed number of bytes. The data owner uploads the file along with meta data into database, with the help of this metadata and its contents, the end user has to download the file. The uploaded file was in encrypted form, only registered user can decrypt it. After the data has been encrypted, it can be spitted as different files. Process splitting can also be sectorized by the data owner. After splitting the process can become the ready state to go for storage sector. Cloud is used as a storage sector here.

Secure Cloud Storage: A secure cloud storage system implies that an unauthorized user or server cannot get the content of stored messages. The cloud storage with dependable server is defined. Finite number of server can be declaimed. The distributed systems are used for storage. There are two main reasons for using distributed systems and distributed computing. First, the very nature of the application may require the use of a communication network that connects several computers. For example, data is produced in one physical location and it is needed in another location. And then second, there are many cases in which the use of a single computer would be possible in principle, but the use of a distributed system is beneficial for practical reasons. For example, it may be more cost-efficient to obtain the desired level of performance by using a cluster of several low-end computers, in comparison with a single high-end computer. A distributed system can be more reliable than a non-distributed system, as there is no single point of failure. Moreover, a distributed system may be easier to expand and manage than a monolithic uni-processor system. Data owners can store their files in this secure cloud storage system, for the purpose of data forwarding process. The required data can be forwarded to the user. Forwarding process can be declaimed as secure data forwarding functioning. Target user must have the retrieval power for the transferring process.

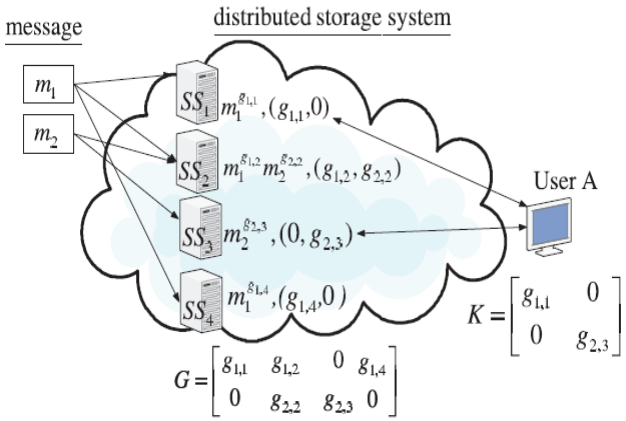

Figure 4: Distributed Cloud Storage System

The Fig 4 shows the system model of distributed cloud storage, which consists of users n, storage servers SS1; SS2; . . . ; SSn, and m key servers KS1;KS2; . . . ; KSm. The distributed storage servers provide storage services and key servers provide key management services. The servers perform all the operations independently. In the cloud storage, user A can encrypts his message M and dispatches it to different storage servers. A message is encoded as a codeword, which is a vector of symbols, and each storage server stores a codeword symbol. A message M is decomposed into k blocks m1;m2; . . .;mk and has an identifier ID. User A encrypts each block mi into a ciphertextCi and sends it to v randomly chosen storage servers. Upon receiving ciphertexts from a user, each storage server linearly combines them with randomly chosen coefficients into a codeword symbol and stores it. The storage size in each storage server does not increase because each storage server stores an encoded result (a codeword symbol), which is a combination of encrypted message symbols. To forward the data from user A to user B then, the user A forwards the message with an identifier ID stored in storage servers to user B such that B can decrypt the forwarded message by the secret key provided by the server.

Cloud Information Accountability: The main concern one should have when choosing a provider is security. Most of the providers will boast that they use secured file transfer with AES encryption. But, consider thinking twice if going to use open a free cloud storage account with an unknown provider.Owner can permit access or

deny access for accessing the data. So users can able to access his/her account by the corresponding data owner. If owner does not allow, user can't able to get the data. The goal of authentication is to identify a user either directly or indirectly. Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks, authentication is commonly done through the use of login passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially or is registered by someone else, using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password.There are many possible ways of authentication available. Some of them are passwords, host-based authentication, physical tokens and biometrics. The way in which someone may be authenticated fall into three categories, based on what are known as the factor of authentication: Something the user has, something the user knows, something the user is. Each authentication factor covers a range of elements used to authenticate or verify a person's identity prior to being granted access, approving a transaction request, signing a document or other work product, granting authority to others and establishing a chain of authority.

Successful Retrieval: The splitted files are merged when the user request for the file they want to the provider. The provider can decide whether to provide the file which has been requested. When the access is granted the file which has been stored in distributed server by splitting the file in to several documents are retrieved by using the secret key which has been generated by using the keg generation algorithm. The file which has been retrieved from different distributed clouds is merged together for the users downloading purpose. The file has to be decrypted, decoded and then forwarded to the client. The function of this module can be integrated with decrypt, decode and forwarding. The authorized party however is able to decode the cipher text using decryption algorithm that usually requires a decryption secret key. AES algorithm is used to decrypt the cipher text. Process retrieval from the cloud storage operation can be performed in this module. Search and select the process which is need by the user from the secure cloud storage.The Authorized users can download the file from cloud database only after the merging and decryption gets over.

6. Experimental Analysis:

The performance of the privacy preserving authentication protocol (PPA) is get analysed with the shared authority based privacy-preserving authentication protocol (SAPA). The access control, storage space, security and usability of PPA protocol is compared with the SAPA protocol and analysed based on the size of the files and number of trials. When a file with 1Mb is used, the security is very low in SAPA compared to PPA. Because the PPA protocol involves 2-level password generation and erasure code whereas on the other hand the SAPA protocol only has proxy re-encryption. The other factor such as usability storage space and access control has some moderate changes based on the size of files. The security of the stored files remains at the same level of all the trials with 5 MB,50 MB and 200 MB. The storage space is consumed less in PPA due to splitting and zipping of the files. So the overall access control is good in PPA and is efficient compared to SAPA. The comparison of PPA and SAPA protocols for security, usability, storage spaces and access control is shown in the following graphs:

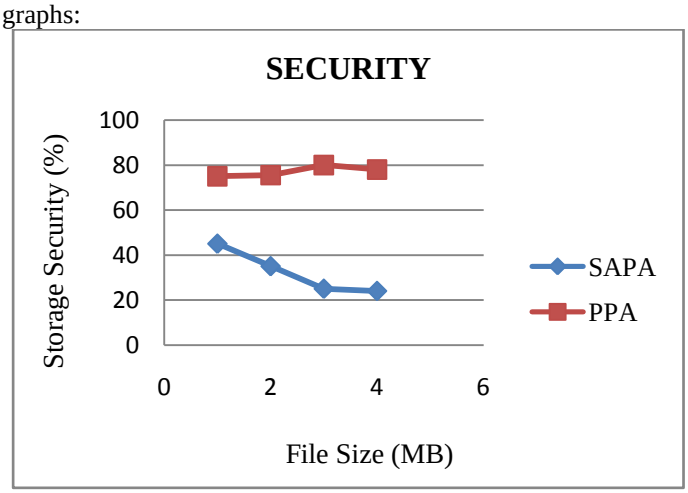

Figure 5: Security

In fig 5 the analysis for security of SAPA and PPA protocols are compared by means of the size of the files. Even when the size of the file increases the security in PPA is maintained. In fig 6 the analysis for usability of SAPA and PPA protocols are compared by means of the size of the files and the result varies when the size of the file get changed.

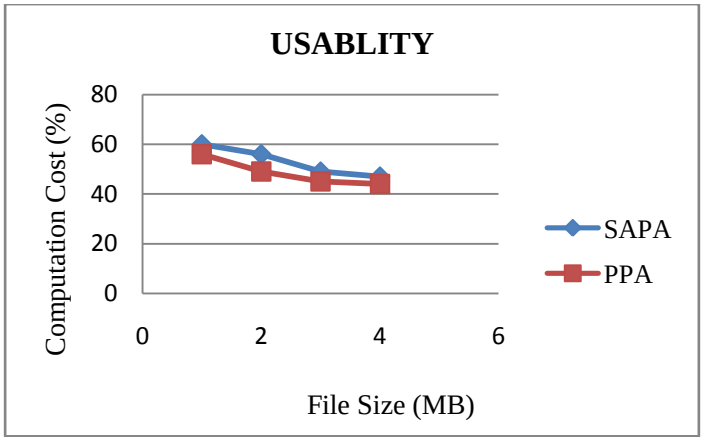

Figure 6: Usability

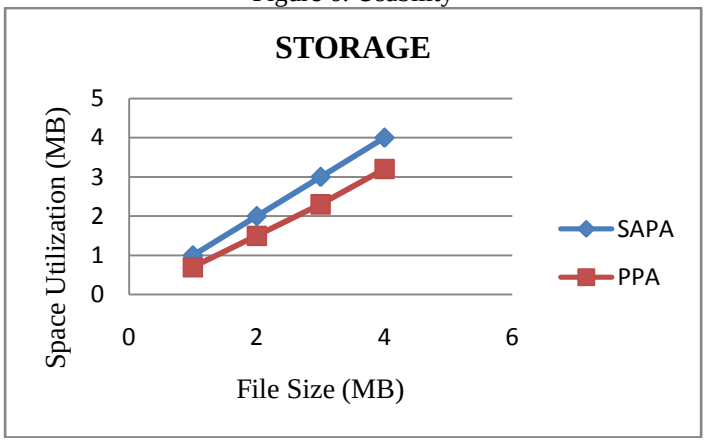

Figure 7: Storage Space

In fig 7 the storage of SAPA and PPA protocols are compared by means of the file size. The PPA protocol provides better and efficient storage space as the files are splitted.

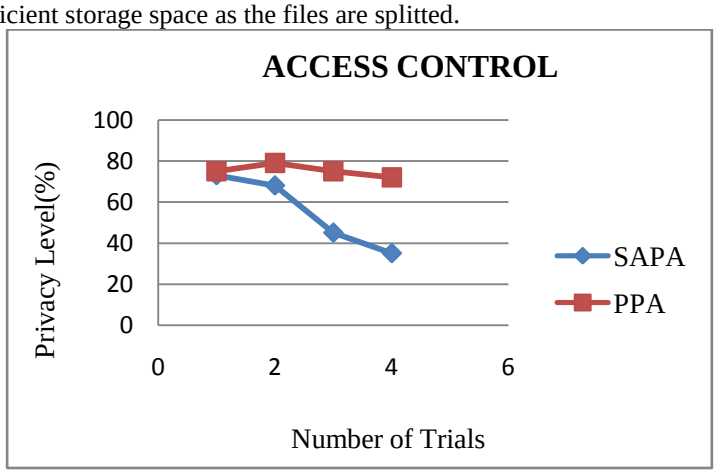

Figure 8: Access Control

In fig 8 the trials have been taken to compare the access control of both SAPA and PPA protocols. Due to 2-level password generation PPA provides better security. The performance of the proposed protocol is get analysed with the existing system shown in table 1.

Table 1: Performance Analysis

Operation	Existing System	Proposed System
Entities	The entities are owner, proxy and receiver	The entities are user (owner, receiver) and distributed server.
Technique Used	Proxy re-encryption is used.	Erasure code is used to provide security.
Access Permission	Created by private key generator (PKG) hence owner has less access to the file.	Created by owner of the file itself and can decide to provide permission.

Key Escrow Problem	Secret key is generated by PKG hence key escrow problem.	Secret key is generated by user and hence no key escrow problem.
Unidirectional	Does not exist	Cipher text are transferred only in one direction

User and distributed cloud storage are the entities of the proposed system in which the file of the owner is spitted and saved in distributed severs by which the security has been improved compared to the previous protocol. Owner can decide the access permission and the key are also provided by the owner on the request from the user.

7. Conclusion:

The Proposed Scheme shared attribute-based privilege control scheme to address the user privacy problem in a cloud storage server. Using multiple authorities in the Cloud Computing system the proposed scheme achieves not only fine-grained privilege control, but also anonymity while conducting privilege control based on users' identity information. User privacy is enhanced by anonymous access rests to privately inform the cloud server about the users' access desires. Forward security is realized by the session identifiers to prevent the session correlation. It indicates that the proposed scheme is possible applied for enhancing privacy preservation in cloud applications.

8. References:

1. H. Liu, H.Ning, Q. Xiong and L.T. Yang "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing," "IEEE Parallel and Distributed Systems, vol.99, 2014.
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. K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," IEEE Transactions onParallel and Distributed Systems, 2012.
4. Q. Wang, C. Wang, K. Ren, W. Lou and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.
5. C. Wang, K. Ren, W. Lou, J. Lou, "Toward Publicly Auditable Secure Cloud Data Storage Services", IEEE Network, vol. 24, no. 4, pp. 19-24, 2010.
6. L. A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," IEEE Transactions on InformationForensics and Security, vol. 8, no. 2, pp. 402-413, 2013.
7. X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions onParallel and Distributed Systems, 2012.
8. S. Grzonkowski and P. M. Corcoran, "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking," IEEE Transactions on Consumer Electronics, vol. 57, no. 3, pp.1424-1432, 2011.
9. M. Nabeel, N. Shang and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," IEEE Transactions on Knowledgeand Data Engineering, 2012.
10. S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," IEEE Transactions onDependable and Secure Computing, vol. 9, no. 4, pp. 556-568, 2012.
11. Y. Xiao, C. Lin, Y. Jiang, X. Chu, and F. Liu, "An Efficient Privacy-Preserving Publish-Subscribe Service Scheme for Cloud Computing," in Proceedings of Global Telecommunications Conference (GLOBECOM 2010), December 6-10, 2010.
12. H. Y. Lin and W. G. Tzeng, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding," IEEE Transactions onParallel and Distributed Systems, vol. 23, no. 6, pp. 995-1003, 2012.