International Journal For Technological Research In Engineering
Volume 3, Issue 7, March-2016 *ISSN (Online): 2347 - 4718*

PROPOSING CLOUD STORAGE USING FUZZY AUTHORIZATION

Jeyageetha.V[1], P.Mownika[2], P.Serakha[3], S.Shanmugha Priya[4]
[1]Assistant Professor, Department of CSE, Nandha College of Technology, Erode-638052
[2,3,4]Student, Final year CSE, Nandha College of Technology, Erode-638052

ABSTRACT: Cloud storage is data storage where the digital data is stored in logical storage disc, the physical storage is in across multiple servers and the physical environment is typically owned and managed by the hosting or the service provider. Cloud storage provides services as an additional layer of data privacy for the precious and non-replaceable files. Backups are kept in a secure location that is physically removed from the originals or the source location. Storing confidential or sensitive information of the individuals or the business data in the cloud is often more secured than storing it local storage device. A new secure authorization scheme for cloud storage providing file divergence patience is called fuzzy authorization. A secret key associated with one attribute set can be applied to another attribute set through proper adjustment as long as the two attribute sets share certain amount of overlap. The security analysis shows that proposed N-FA (Novel Fuzzy Authorized) scheme provides a thorough security of outsourced data, including confidentiality, Veracity secure access control, implemented the cryptographic part and simulated the protocol based on Third Party Auditor (TPA). Novel Fuzzy Authorized scheme reduces the storage consumption compared to other similar possible authorization schemes. It also emphasizes that our scheme could efficiently achieve distance tolerance and grasp fuzzy authorization in practice research study. In addition, enabling public review ability for cloud storage is critical importance so that the users can route to a TPA to check the trustworthiness of outsourced data and be unstressed. This proposed system supplies the secure storage system in cloud environment and sustaining privacy-preserving public auditing. It can be enhanced as the result to enable TPA to perform inspects for multiple users concurrently and efficiently.

Key word: Cloud Storage, secure authentication, fuzzy authentication.

I. PROBLEM DEFINITION

In existing system, the operations are carried out in the following aspects.

- Data Owner: Data owner an entity who stores the data inside cloud storage and wishes to employ the cloud application services to process the data. A data owner must register with cloud storage provider and must be logged-in in order to upload the data or access the data or authorize the data.
- Application Service Provider: Entity to be authorized to access the data which is stored in cloud storage. The application software be located in vendor's system or cloud and can be accessed by users through a web browser or special purpose client software. For example, PDFMerge is an online tool which can be used to merge several PDF files into one PDF file. With proper authentication, PDFMerge fetches the source PDF files from the cloud storage. As a result, uploading files from data owner's local device is avoided.
- Cloud Storage Provider: Entity which supplies storage as a service to its clients and also provides access application programming interfaces to ASP when ASP holds a valid access token.
- Application store (AS): Entity with which ASP must be registered to ensure it self's integrity and authenticity. Google Chrome Web Store is a typical application store.
- Data owner encrypts his data with a random symmetric key KE and encrypts KE with our modified CP-ABE scheme. Owner encapsulates cipher text of KE and cipher text of data as an archive and stores the archive in the CSP. When owner needs to share data with ASP, he/she and CSP join together o issue ASP the indirect secret shares of file attributes while AS and owner collaborate to issue the indirect secret shares of application attributes. In this study, an indirect share contains a genuine secret share as its exponent or a part of its exponents.

II. LIMITATION OF EXISTING SYSETEM

Different kinds of access mechanism are not applied and so different client applications with varying processing capabilities need to execute the cloud data in same manner.

- Time limit is not discussed and so client like to access the data in same tariff for the whole period.
- Correlated Authentication aspects with combination of both cloud storage provider, application service provider and end user is not considered.

III. PROPOSED SYSTEM

The cloud storage system availability, it is natural to assume that every entity trusts the proposed protocol and execute the protocol honestly, although the entities do not trust each other. Despite we cannot ensure every entity not to exploit the threats to attack the system, we consider the following possible threats as adversary models. In addition with all the existing system mechanism, a correlated Authentication aspect with combination of the cloud storage provider, application service provider and end user is also considered.

In addition, time limit is provided to end user to access the Application Service Providers (ASPs). So at different time intervals, different kinds of tariffs can be applied to end users to access the service. Likewise, the security aspects provided by the cloud storage provider is also taken by ASPs to increase the security more. In addition, trusted third party authentication mechanism is included.

- Different kinds of access mechanism are applied and so different client applications with varying processing capabilities need to execute the cloud data in same manner.
- Time limit is set and so client likes to access the data in different levy for diverse time periods.
- Correlated Authentication aspects with mixture of both cloud storage provider, application service provider and end user is also considered.
- Trusted third party authentication with no security violation is included

IV. PROBLEM EXPLANATION

Data Reduplications eradicates the redundant data by storing only the single copies of data. It uses the convergent encryption technique to encrypt the data with the convergent key. It also provides Differential Authorized duplicate check, so that only authorized user with specified privileges can perform the duplicate check. The concept de-duplications save the bandwidth and reduce the storage space. It also eradicates the duplicates of data in the cloud storage.

Fuzzy authorization (FA) which carries out a legible file-sharing scheme between an owner who stores the data in one cloud party and applications which are registered within another cloud party. The security analysis shows that proposed N-FA (Novel Fuzzy Authorized) scheme provides a thorough security of outsourced data, including confidentiality, integrity and secure access control.

Novel-Fuzzy Authorized approach reduces the storage consumption compared to other similar possible authorization schemes.

- CSP is trusted to provide storage services properly but may intend to access owner's data illegally. CSP may take advantage of the indirect shares that it possesses and query the other indirect shares so as to reconstruct the top secret.
- ASP may try to decrypt the unauthorized files by utilizing the previous indirect shares issued to him. ASP is allowed to query for the indirect shares that he/she does not possess.
- AS which is involved in issuing the indirect application secret shares may try to access owner's data in the name of ASP. Since it knows about partial indirect shares of application attributes, he/she may query about the indirect shares of file attributes and try to obtain the complete indirect shares of application attributes.
- An adversary owner may personate other owners to contribute the gra1 part for each attribute share.
- Targeting on the secret keys and access tokens, general network attacks might be launched by Internet hackers.

V. OBJECTIVES OF PROPOSED SYSTEM

Data Reduplication eradicates the redundant data by storing only the single copies of data. It uses the convergent encryption technique to encrypt the data with the convergent key. It also provides differential authorized duplicate check, so that only authorized user with specified privileges can perform the duplicate check. The concept de-duplications save the bandwidth and reduce the storage space. It also eradicates the duplicates of data in the cloud storage. FA which carries out a legible file-sharing scheme between an owner who stores the data in one cloud party and applications which are registered within another cloud party. The security analysis shows that our N-FA (Novel Fuzzy Authorized) scheme provides a thorough security of outsourced data, including confidentiality, integrity and secure access control. Novel-Fuzzy Authorized approach reduces the storage consumption compared to other similar possible authorization schemes.

VI. NEED FOR PROPOSED SYSTEM

The important issue is that more than one access token or secret key is required for access control of files. Let us assume one person have hundreds of pdf file there in cloud storage than person want to merge his file, first person want to download his file in cloud storage then after merged the pdf with application provider. At file need a secret key for accessing the pdf than only merged the pdf. That is very difficult to person than only we are using fuzzy authorization in cloud storage, in the system secret key create only one users not every pdf file so here access control be reduced compared to last system. Cloud storage is widely used for storing large data from various users at different place, but cloud storage provider has a lot of issues like data missing, security, access control and confidentiality. To overcome these issues, novel fuzzy authorization scheme in cloud storage is needs to be proposed. In this technique to enable an application registered with one cloud account to access data files in own cloud account.

VII. SYSTEM METHODOLOGY

Data security is one of the biggest concerns in adopting Cloud computing. In Cloud environment, users remotely store their data and relieve themselves from the hassle of local storage and maintenance. However, in this process, they lose control over their data. Existing approaches do not take all the facets into consideration viz. dynamic nature of Cloud, computation & communication overhead etc. In this study propose a Data Storage Security Model to achieve storage correctness incorporating Cloud's dynamic nature while maintaining low computation and communication cost. The only kind of guarantee is based on the level of trust between the cloud customer and the cloud provider and on the contractual regulations made between them such as SLAs, applicable laws, and regulations of the involved jurisdictional domains. But even if the relation and

agreements are perfectly respected by all participants, there still remains a residual risk of getting compromised by third parties. To solve this intrinsic problem, multiple distinct clouds executing multiple copies of the same application can be deployed. Instead of executing a particular application on one specific cloud, the same operation is executed by distinct clouds. By comparing the obtained results, the cloud user gets evidence on the integrity of the result. In such a setting, the required trust toward the cloud service provider can be lowered dramatically. Instead of trusting one cloud service provider totally, the cloud user only needs to rely on the assumption, that the cloud providers do not collaborate maliciously against herself.

1 SECURITY PROSPECTS BY MULTI CLOUD ARCHITECTURES

The basic underlying idea is to use multiple distinct clouds at the same time to mitigate the risks of malicious data manipulation, disclosure, and process tampering. By integrating distinct clouds, the trust assumption can be lowered to an assumption of non-collaborating cloud service providers. Further, this setting makes it much harder for an external attacker to retrieve or tamper hosted data or applications of a specific cloud user. The idea of making use of multiple clouds has been proposed by Bernstein and Celesti. However, this previous work did not focus on security. Since then, other approaches considering the security effects have been proposed. These approaches are operating on different cloud service levels, are partly combined with crypto-graphic methods, and targeting different usage scenarios. A model of different architectural patterns is introduced for distributing resources to multiple cloud providers. This model is used to discuss the security benefits and also to classify existing approaches. This model distinguished the following four architectural patterns:

Replication of applications allows to receive multiple results from one operation performed in distinct clouds and to compare them within the own premise. This enables the user to get evidence on the integrity of the result.

Partition of application System into tiers allows separating the logic from the data. This gives additional protection against data leakage due to flaws in the application logic.

Partition of application logic into fragments allows distributing the application logic to distinct clouds. This has two benefits. First, no cloud provider learns the complete application logic. Second, no cloud provider learns the overall calculated result of the application. Thus, this leads to data and application confidentiality.

Partition of application data into fragments allows distributing fine-grained fragments of the data to distinct clouds. None of the involved cloud providers gains access to all the data, which safeguards the data's confidentiality.

Each of the introduced architectural patterns provides individual security merits, which map to different application scenarios and their security needs. Obviously, the patterns can be combined resulting in combined security merits, but also in higher deployment and runtime effort. The following sections present the four patterns in more detail and investigate their merits and flaws with respect to the stated security requirements under the assumption of one or more compromised cloud systems.

Advantages of cloud storage such as ease of accessibility, in-time syncing and less physical space consuming, etc., have motivated more and more people to adopt cloud storage services. In the meantime, cloud application services are boosting as well. As a result, the demand of inter operations and authorizations between cloud storage service providers and cloud application service providers (ASPs) becomes more and more urgent. For example, a data owner stores several PDF files inside Justcloud, which is the top one cloud storage service provider. Later

2 PROPOSED ALGORITHM

Data owner: an entity who stores his/her data inside cloud storage and wishes to utilize cloud application services to process the data. A data owner must register with cloud storage provider and must be logged-in in order to upload, access data or authorize.

Algorithm:

Input: Original Data File

Output: Cipher text file

Steps:

Step1: Generate Random Symmetric key (KE) under the access tree ť

Step2: Encrypt owner data file using modified CP-ABE with symmetric key (KE)

Step3: Archive / Encapsulate the cipher text of key (KE) and cipher text of data

Step4: Store the encapsulated/archived cipher text data in the CSP

Application Service Provider: an entity to be authorized to access cloud storage data. It is an application software resides in vendor's system or cloud and can be accessed by users through a web browser or a special purpose client software. For example, PDF Merge is an online tool which can be used to merge several pdf files into one pdf file. With proper authorization, PDF Merge fetches the source pdf files from cloud storage. As a result, uploading files from data owner's local device is avoided.

Algorithm: Decrypt(CT, SK, x)

Input: Decrypt Node , Cipher text (CT), Secret Key (SK)

Output: Decrypted data (plain data)

Steps:

Step1: x is a leaf node of access tree and i is the attribute attached to x

Step2: decrypt (CT,SK,x)

Step3: $e(D_i,C_x)/e(D'_i, C'_x) = e(g_1^{ra} H(i)^i, g_2^{px(0)}/e(H(i)^i, g_2^{px(0)})$

Step4: stores the result $fz= (f_{z0}, f_{z1,\ldots} f_{z\,n-1})$, $f_{zi}=e(g_1,g_2)^{raPzi(0)}$

Cloud Storage Provider: an entity which supplies storage as a service to its clients and also provides access application programming interfaces to ASP when ASP holds a valid access token. Drop box and Just Cloud mentioned previously are examples of such entity.

Algorithm:
Input: security parameter k
Output: public key
Steps:
Step1: Choose bilinear map (e : $G_1 * G_2 \rightarrow G_T$ of prime order q
Step2: Generate g_1,g_2
Step3: generate random exponent ß
Step4: publish the public key CPK= (G_1,G_2,g_1,g_2, $h=g_1^{ß}$,$f=g_2^{1/ß}$)
Step5: keep the secret key CSK(CPK= (ß)
The importance of fuzzy search has received attention in the context of plaintext searching in information retrieval community. They addressed this problem in the traditional information-access paradigm by allowing user to search without using try and approach for finding relevant information based on approximate string matching. The approximate string matching algorithms among them can be classified into two categories: on-line and off-line. The on-line techniques, performing search without an index, are unacceptable for their low search efficiency, while the off-line approach, utilizing indexing techniques, makes it dramatically faster.
The proposed algorithm analyze from the perspectives of internal and external adversaries. For internal adversaries, all entities in the system are considered to be trusted, in the sense that they can exploit threats to subvert authorization control and data security, but still honestly follow the protocol. External adversaries may not run the protocol but try to launch general attacks to violate data security.

VIII. CONCLUSION

To ensure the security and dependability for cloud data storage under the aforementioned adversary model, we aim to design efficient mechanisms for dynamic data verification and operation and achieve the following goals:

- Storage correctness: to ensure users that their data are indeed stored appropriately and kept intact all the time in the cloud.
- Fast localization of data error: to effectively locate the mal- functioning server when data corruption has been detected.
- Dynamic data support: to maintain the same level of storage correctness assurance even if users modify, delete or append their data files in the cloud.
- Dependability: to enhance data availability against Byzantine failures, malicious data modification and server colluding attacks, i.e. minimizing the effect brought by data errors or server failures.
- Lightweight: to enable users to perform storage correctness checks with minimum overhead.

In this experimental study, the existing system is describing the problem of secure authentication for storage in cloud. In this thesis, proposed FA which carries out a legible file-sharing scheme between an owner who stores the data in one cloud party and applications which are registered within another cloud party. The security analysis shows that proposed N-FA (Novel Fuzzy Authorized) scheme provides a thorough security of outsourced data, including confidentiality integrity and secure access control. Novel-Fuzzy Authorized approach reduces the storage consumption compared to other similar possible authorization schemes. It also asserts that our scheme could efficiently achieve distance tolerance and realize fuzzy authorization in practice research study. This work mainly addresses the reading authorization issue on cloud storage. And it results to enable the TPA to perform audits for multiple users simultaneously and efficiently

IX. FUTURE ENHANCEMENTS

In this paper problem of data security in cloud data storage, this is essentially a fuzzy storage system. To ensure the secure of users' data in cloud data storage, proposed an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append. To rely on erasure-correcting code in the file distribution preparation to provide redundancy parity guarantee the data dependability. By utilizing the heterogenic security with distributed verification of erasure coded data, proposed scheme achieves the integration of storage correctness insurance and data error localization, i.e., whenever data storage has been detected during the storage correctness verification across the distributed servers, we can almost guarantee the simultaneous identification of the misbehaving server(s). Through detailed security and performance analysis and show that proposed scheme is highly efficient and resilient to Byzantine failure, malicious data modification attack, and even server colluding attacks. The following enhancements are should be in future.
The application if developed as multi web services, then many applications can make use of the records.

- Search semantics that takes into consideration conjunction of fuzzy set data, sequence of fuzzy set data, and even the complex natural language semantics to produce highly relevant authentication search results
- Search and data store ranking that sorts the searching results according to the relevance criteria.
- The data integrity in cloud environment is not considered. The error situation can be recovered if there is any mismatch.

The web site and database can be hosted in real cloud place during the implementation.

REFERENCES

[1] Agudo, "Cryptography goes to the cloud," in Proc. Workshop Secure Trust Compute., Data Manage. Appl., 2011, pp. 190–197
[2] P. Arias-Cabarcos, F. Almen arez-Mendoza, A. Marn-Lopez, D. Dıaz-Sanchez, and R. Sanchez-Guerrero, "A metric-based approach to assess risk for "on cloud" federated identity management," J. Netw. Syst.Manage., vol. 20, no. 4, pp. 1–21, 2012.
[3] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute-based encryption," in Proc. IEEE Symp. Security Privacy, 2007,pp. 321–334.

[4] Jøsang and S. L. Presti, "Analyzing the relationship between risk and trust," in Proc. 2nd Int. Conf. Trust Manage., Mar. 2004, pp. 135–145.
[5] T. Grandison and M. Sloman, "A survey of trust in internet applications," IEEE Common. Survey. Tutorials, vol. 3, no. 4, pp. 2–16, Fourth Quarter 2000.
[6] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Compute., vol. 16, no. 1, pp. 69–73, Jan./Feb. 2012.
[7] P. Samarati, and S. D. C. di Vimercati, "Data protection in outsourcing scenarios: Issues and directions," in Proc. 5th ACM Symp.Inf., Compute. Common. Security, 2010, pp. 1–14.
[8] G. Schryen, M. Volkamer, S. Ries, and S. M. Habib, "A formal approach towards measuring trust in distributed systems," in Proc. ACM Symp. Appl. Compute., 2011, pp. 1739–1745.
[9] Tassanaviboon and G. Gong, "OAuth and ABE based authorization in semi-trusted cloud computing," in Proc. 2nd Int. Work shop Data Intensive Compute. Clouds, 2011, pp. 41–50.
[10] J. Xu, E.-C. Chang, and J. Zhou, "Weak leakage-resilient client side reduplication of encrypted data in cloud storage," in Proc. 8th ACM SIGSAC Symp. Inf., Compute. Common. Security, 2013, pp. 195–206.

