International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 6, Issue 4, 2019

# A Secure Cloud Storage Link Sharing Mechanism

**Shu Yun Lim[a], Munirah Yusoff[b], Paridah Daud[c], Alfonso Johan[d], Noor Azma Binti Ismail[e],** [a,c,e]Faculty of Business and Technology, UNITAR International University, Selangor Darul Ehsan, Malaysia, [d]ICT Services, UNITAR International University, Selangor Darul Ehsan, Malaysia Ehsan, Malaysia, [b]Odekan Technologies PLT, Cyberjaya Selangor, Malaysia,
Email: lim_sy@unitar.my, munirah.yusoff@team.odekan.tech, paridah69@unitar.my, alfonso.johan@unitar.my

Cloud storage offers a convenient way of keeping files on an external server and also sharing them with other users publicly. There can be a risk of data leakage when sensitive information is being used without permission. In this untrusted cloud environment, anyone could share documents that are owned by someone else. This problem of loss of data ownership becomes a major hindrance of cloud adoption. This project examined the weaknesses of existing link sharing mechanisms in two cloud storage providers, namely Dropbox and Google Drive. The result shows security weaknesses in each provider may lead to data breaches without user awareness. Hence, a secure cloud storage link sharing mechanism using ticket is proposed to improve the security of link sharing. This secure mechanism is able to resolve existing private-URL sharing and secret-URL sharing security issues.

**Key words:** *cloud storage, link sharing, security.*

## Introduction

Cloud Storage enables data sharing capabilities and it is maintained and managed by Cloud Storage Providers (CSP). They are also responsible to protect physical environment and ensure that the data stored in the cloud are available and accessible. In recent years, the usage of cloud storage services has been increasing dramatically as storing and accessing the data can be conducted anywhere and at any time. As a critical component in the cloud computing model, mostly these resources are accessed on a pay-per-use or subscription basis based on user need. Individual consumers use it to store music, videos, and photo and share documents online with friends while in business, the major benefits are in data backup and disaster recovery due to the greater accessibility and reliability. It also reduces company's operational

costs and improves cash flow as there is no need to purchase any hardware for the application development and maintenance.

Storing sensitive information and sharing it with others are the biggest concerns in cloud storage. The security of data being stored and transferred in the cloud is in question because it is beyond users' control. The other challenge is the security concern regarding the sharing of files and folders. Due to limited ability to manage who can share content externally, with what permission and to which categories of use (e.g. restricted to registered users vs. via an open file link), the data stored could be exposed to the entire Internet. The CSPs make sharing easy to use through link sharing mechanisms such as Public Sharing, Secret-URL Sharing and Private Sharing, but several weaknesses in sharing mechanisms still exist.

This research aims to determine the security weaknesses in major cloud storage and the potential of link sharing mechanisms that may result in data breaches without users' awareness. The proposed mechanism allows users to manage and share their data over untrusted Cloud Storage Providers (CSP) via a secure link sharing mechanism. Since users require a certain degree of control to ensure data confidentiality and integrity, securing the link sharing mechanism is the utmost priority. The link sharing mechanism is based on the 'ticket' approach whereby only authorized users have access to the data therefore preventing the data being shared without the data owner's permission.

## Literature Review

### *Analysis of existing link sharing mechanism*

Existing link sharing mechanisms in two cloud storage providers, namely (Dropbox, 2019) and Google Drive (2019) were examined. Generally, it is difficult to control the privacy once the file or folder is made public on the Internet. Some of the weaknesses are:

- No unique identification number assigned to users invited to share the file or folder. The owner has difficulty to track additional users who have access to the file.
- The invitation link that may be exposed to another person. There is no authentication to prove that the invitation link is used by the intended user only.
- The intended users can sign in with a different email account apart from the email used by the owner to invite him or her to access the shared resource.
- The links can be shared with anyone even if they do not have a Cloud Storage account. The owner is unable to keep track of file access activities by user with or without invitation.
- Unauthorized user who gains access to the file via link invitation, also have all the privileges or permissions that the owner gave to the intended user.

***Related works***

Previous researchers (Chachapara and Nigam, 2015), (Nkemakolam et al., 2018) proposed a framework, a security mechanism of generating a key, sharing a key and validating the use of that key for file access. The framework used cryptography to generate a secure key that can be shared among users. Mobile technology is used to contact service providers and generate a key as when needed. Cloud Service Providers (CSPs) generate links for selected files and ask for authentication ticket from owner of the file. The link is passed to the mobile number provided by the owner of the file. Encryption and decryption are done based on the number of accesses done on the said file using provided key. If the number of accesses are equal, the CSP returns a ticket with the response that the link has expired. However if the number is less, than the CSP will perform the decryption of the key using the same algorithm as for encryption. The ticket is a unique authentication password that will validate the identity of the owner. If the authentication ticket is valid, then the service provider will experience success with requesting details on file for which a key needs to be generated. The key generation is done by taking a secret code from a user and generating a 128-bit key using an AES algorithm. Once all details are available service providers will generate links containing selected access on selected files. Through a simulation, the authors have tried to establish the secure sharing link that allows cloud users to share files without also having internet connection.

The architecture proposed by Shani Raj et al used a policy-based encryption technique. An access key generated for the user is based on access policies assigned to each user along with the attributes. The data stored in the cloud is encrypted using a key generated on the access permissions assigned to the data and attributes of the owners who share their data. The performance evaluation shows that a user can share data with others in the system. It also showed groups are capable of storing and sharing their data as well. The system also supports efficient file revocation and policy changing.

Another work is Cloud Information Accountability (CIA) Framework (Alhat et al., 2014), (Hye, 2012). The CIA Framework conducts automated logging and distributed auditing of relevant access performed by any entity, carried out at any point of time for any cloud service provider. One of the modules in CIA is Random Set Generation and Verification which is a random number set generated for every user during the registration phase itself. The user must enter the random number set which will allow the user to download the data. The user is required to provide the random number when accessing the account and have it verified by the server. Access is only granted to the account if the verification is positive. This approach allows the data owner not only audit his content but also enforces strong back-end protection if needed.

Wang, B., et al. (2013) introduced a security-mediator (SEM), which is able to generate verification metadata (i.e., signatures) on allowed blocks of data for an owner before these data are outsourced to the cloud. Every block will be processed with blinding technique and the block blinded versions are sent to the SEM. The SEM then computes a blind signature with its private key and returns this blind signature back to the data owner. The data owner transforms this blind signature to obtain the actual signature on the original block and uploads all the data and corresponding signatures to the cloud server. The data is in small blocks and each have a signature that enable a public verifier to check data integrity by retrieving only a random combination of all the blocks instead of retrieving the entire cloud data from the cloud server. This operation ensures the data privacy, which even the SEM is not able to reveal the content of data it blindly signed before or link a data owner to the data or signatures stored on the cloud.

## Proposed Mechanism

### *Overview*

The proposed mechanism to secure file sharing in Cloud Storage is based on weaknesses discovered in existing cloud storage service. The mechanism consists of four entities; user, intended user, cloud provider, and a Link Authenticator to protect the file from unauthorized user. The user uploads data to the cloud for sharing and considers that the file stored is managed and modified by only a single data owner. Using an invitation method, a link is sent to the intended users that enables them to access the uploaded data. However, the intended users are not allowed to re-share the link since their credentials have been attached to the link.

The cloud provider provides data storage and sharing services to the users. The Link Authenticator provides security services to the user that contains an authentication ticket attached to the link before these data are outsourced to the cloud. In this mechanism, we assume that the communication channel between the cloud server and the verifier is authenticated (Cong et al., 2009), (Obialor, 2017). All entities in the proposed mechanism, the users or servers, have a secret key that is shared only by the authentication server. To obtain services from the cloud storage a user must obtain a ticket granted by the authentication server. The ticket contains a user credential with the secret key belonging to the requested service. The user presents this ticket to the cloud server, which verifies ticket authenticity. This ticket cannot be forged nor can it be tampered with since the ticket is generated for the intended user only. The procedure for obtaining and using tickets is as follows:

- Authentication – An authentication ticket is obtained from authentication server if the user wants to access and use the cloud provider services. The ticket requires some section of metadata (users and file) so that proper credentials can be attached to the link sharing.

With this, others won't be able to access that file since the link contains an expiration and user validation. It also will prove that the authentication message has not been modified in transit.

- Verification - The authentication return success if the credentials of the users are valid. Timestamps within acceptable time (~5 minutes) must be synchronized between two computers to be considered as authentic.

***Requirements of Data Sharing in the Cloud***

To enable data sharing in the cloud and easily managing the user access, it is important that only authorized users can get access to data. Summary of ideal requirements for data sharing in the cloud as listed below.

- Enable the data owner to specify a group of users that are allowed to gain access to his or her data. Each intended user may have multiple groups with different credentials.
- Restrict the data access to the data owner and the members of the group only. No other user, including the CSPs can access.
- Only the data owner has the rights to revoke access of the data for any member of the group.
- The member of the group should not be allowed to add new user or revoke the rights of current member of the group without the data owner intervention.
- Restrict the link invitation of file to the intended user only. Whoever have the link but not invited by the data owner cannot access it.

Internal policies and procedures to capture and manage metadata must be completed where it should address the following:

- Checking of relevancy and accuracy of metadata
- Ensuring the completeness of metadata
- The metadata required when uploading file into cloud storage systems
- Ensuring consistency in the creation and interpretation of metadata
- Capturing metadata (including the elements to capture, date and time, who captures what element and what tools are used.

In the proposed mechanism, there are two types of metadata; file metadata and access control metadata.

- File metadata: The file metadata contains file size and file ID attached in the file once the file is uploaded to the cloud storage.
- Access control metadata: The access control metadata includes the user's email address and access ID. It is uploaded as a separate file to the cloud storage, which enables the user to renew access control directly on the access control metadata. In other word, for two

data files with the same access control, they will have a different access control metadata, specified by the authentication token.

***Generation of Uniform Resource Locator (URL)***

**Table 1:** Parameters

| Type | Field Name | Size (bits) | Description |
|---|---|---|---|
| User | EmailAddress | 128 | Email address of a user. |
| Access ID | AID | 64 | User Access Identification |
| File ID | FileID | 64 | The alphanumeric sequence identifying a file. |
| Folder ID | FolderID | 64 | The alphanumeric sequence identifying a folder. |
| FileSize | FileSize | 128 | The size that the file or folder is uploaded on the cloud provider. |

To generate the URL for sharing and incorporating the proposed security mechanisms in the link, a unique identifier is required to verify that the user has permission to access the file or folder. A dedicated parameter applying to the metadata were selected to determine what file the intended user can access to a user's cloud storage. Parameters assigned to the file is as shown in Table 1.

Below are detailed features of then URL generated when sharing the file and folder:

1. /metadata

- DESCRIPTION Retrieves file and folder metadata
- STRUCTURE https://provider.com/metadata/<path>
    - *path* The path to the file or folder
    - *provider.com* Depends on which CSP is used
- PARAMETERS *include_membership* A list of members and groups for a shared folder (Contains AID and FID)
- RETURNS The metadata for the file or folder at the given <path>.

2. /metadata/link

- DESCRIPTION Retrieves metadata about a shared link.
- STRUCTURE https://provider.com/metadata/link
- PARAMETERS
    - *link* The URL of the shared link.

- *path* Retrieve the metadata for a specific file or subfolder within the shared link.
- *AID* User Identification used to identify who is the owner or who is applicable to access the file link.

- RETURNS The metadata for the file or folder at the given shared link just like /metadata with some extra fields.

3. /shared_folders

- DESCRIPTION Returns a list of all shared folders the authenticated user has access to or metadata about a specific shared folder.
- STRUCTURE https://provider.com//shared_folders/<shared_folder_id>
- PARAMETERS
  - *shared_folder_id* The ID of a specific shared folder.
  - include_membership Required if *shared_folder_id* is specified. If true, include a list of members and a list of groups for the shared folder.
  - RETURNS A list of shared folders metadata objects, or the metadata for a specific shared folder if the *shared_folder_id* parameter is specified.

The path is "None" for shared folders where the user is no longer in the shared folder access list. The membership field only contains users who have joined the shared folder and does not include users who have been invited but have not accepted. When the active field is false, it means that a user has left a shared folder (but may still rejoin).

**Implementation and Evaluation**

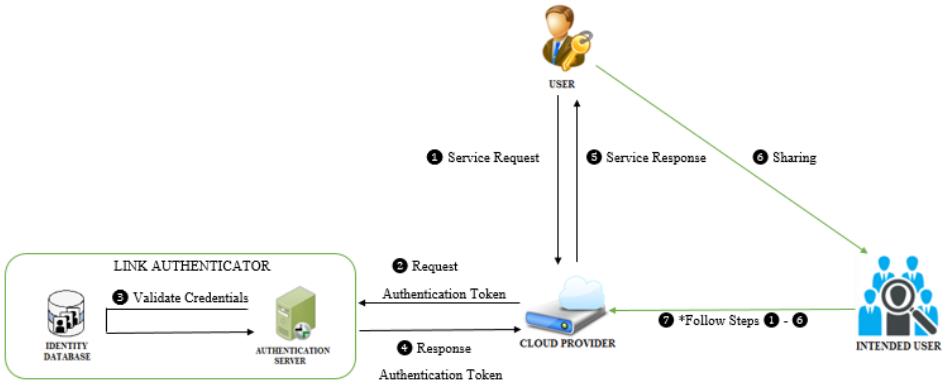
***Design Implementation***

Our proposed link sharing mechanism for cloud applications was designed to ensure that only users who have been granted an authentication ticket and the Access ID can access the resource. It also allows the owner to verify whether the intended user is qualified to access their data. Additional Access ID Authenticator security information:

- Users always use HTTPS when accessing the cloud provider
- Passwords are never sent in clear text from the user
- The user (data owner) can control the intended user access through authentication ticket which prevent from unauthorized re-share
- The user (data owner) can also whitelist/blacklist the intended user to specific file shares.

The details of the components and the mechanism required for communications between these components are explained as below:

**Fig. 1.** A Secure Cloud Storage Link Sharing Mechanism




As illustrated in Fig. 1, the following steps describe the authentication ticket process:

a) The Authentication

1. The user requests to access the cloud provider.
2. The cloud provider then requests an authentication token to validate the user.
3. The authentication server contacts the identity database to validate the user's credentials.
   - Validation is based on the user's email.
   - If the user is registered in the database, the user will be authenticated.
4. The authentication server responds to the cloud provider and issues a security ticket if authentication is successful.
   - Return success with the Access Identification (AID)
   - The security ticket has a short lifespan (8 hours) that is defined by the authentication server.
5. The cloud provider returns the response to the user.

b) Link Sharing

6. To begin sharing a file or folder, the user gains a link generated by the cloud provider and notify link to the intended user.
7. When the data owner enters the intended user's email address, the intended user AID is automatically attached.
8. Once the intended user received the link, the intended user needs to gain the authentication ticket to prove that they are an intended user. Repeats steps 1 to 5 as shown above.

## Security Analysis

### *Data Security*

This section details how the link sharing is secure by the proposed mechanism and controls available to users shared file.

- Fine grained access controls – The use of link authentication ticket and access ID supports the principle of least privilege – granting the minimum access necessary. It prevents any unauthorized access to restricted data while allowing appropriate user and application usage.
- Features security - The proposed solution provides extensive protection features. The link to file contains a credential of the intended user only. The link has restricted its use for a defined period that can prevent from re-share.
- Auditing and reporting – Data owner can track and log all user activity, including both data access and data sharing since the link sharing contains user credentials.

### *Cloud Storage Service Security*

Apart from ensuring data protection, the proposed mechanism also offers a practical defence to some security problems related to cloud storage.

- Replay attacks – Replay attack occurs when an attacker captures and resubmits data (commonly a credential) with the goal of gaining unauthorized access to an asset (Harris and Foreword, 2001). A ticket is used to authenticate individual transactions in addition to sessions to prevent from replay attacks. When users access to the cloud, they are required to provide their credentials, a timestamp, an access ID and the tickets. The tickets are shared between the users and link authenticator servers. The servers allow the users to access to file requests if the data matches.
- Information disclosure – Consider the nature of sharing a file or folder in a cloud platform. It remains private only to data owners, unless the owner begins sharing with others. With the ticket of the intended users to access the file or folder, it blocks other users from accessing the intended user's stored information.
- Elevation of privilege - Usually file sharing user's privileges include viewing and editing files. However, when a user received the file with the privileges they are not entitled to (e.g., user to view-only can access content with view and edit files), can cause an unauthorized access which goes beyond what is necessary for those privileges. The link mechanism prevents this problem with the user credentials, a timestamp, an Access ID and the session tickets, each time the CSPs generate a link to file.

## Conclusion

The proposed mechanism aims to secure user data and to manage who can access the data. Future work includes the implementation of the proposed mechanism to protect file access based on user requirements. Further, the mechanism could be improved by implementing an approval method where owner of a file can approve the invitation of another user and thus be invited to be a shared user of the file.

**REFERENCES**

Alhat Rajendra, Y., Sangale, B.G. & Nilesh, N.T. (2014). Ensuring distributed accountability for data sharing in the cloud. International Journal of Engineering Research & Technology (IJERT), 3(2): 494-501.

Chachapara, K. & Nigam, R.K. (2015). Framework to establish offline file sharing in Application as a service layer in cloud computing. Framework, 6(7).

Cong, W., W.Q., Kui, R. & Wenjing, L. (2009). Ensuring data storage security through a novel third party auditor scheme in cloud computing.

Dropbox, (2019). Available from: https://www.dropbox.com.

GoogleDrive, (2019). Available from: https://www.google.com/drive/.

Harris, S. & Foreword J. (2001). By-Kowtko, CISSP certification all-in-one exam guide: McGraw-Hill Professional.

Hye, M. A. Q. (2012). Exports, imports and economic growth in China: An ARDL analysis. Journal of Chinese Economic and Foreign Trade Studies, 5(1): 42-55.

Nkemakolam, O. E., Chinelo, O. F. & Jane, M. C. (2018). Effect of computer simulations on secondary school students' academic achievement in chemistry in Anambra State. Asian Journal of Education and Training, 4(4): 284-289.

Obialor, M. C. (2017). Effect of government human capital investment on economic growth in Sub-Saharan Africa: Evidence from Nigeria, South Africa and Ghana (1980-2013). International Journal of Asian Social Science, 7(4): 328-339.

Shani Raj, D., Paul, V. & Rahim, N. Multi-Owner data sharing in cloud storage using policy based encryption.

Wang, B., et al. (2013). Storing shared data on the cloud via security-mediator. 2013 IEEE 33rd International Conference on Distributed Computing Systems. IEEE.