A Combined Model to Ensure Complete Security and Reliability in Cloud Computing

Ankit Sharma, Shashank Gupta, Deep Mann, Shakil Akhtar

Abstract— **Cloud Computing is the fastest growing technique in the IT (Information Technology) industry as its main idea is to maximising the capacity and capabilities vigorously without investing in new infrastructure and licensing software. It provides a large amount of storage capacity over the internet but the management and security of the data and services over the cloud is not entirely trustworthy. Because of the lack in trust, most of the businesses are still reluctant to deploy their business over cloud, so security is the major concern in cloud computing and becoming a major issue in the implementation of cloud.**

In this paper, a new framework is proposed which focuses on almost every aspect of security i.e. protection of data from beginning to end, i.e., from cloud owner to user. This work focuses on major four aspects of security, i.e., Confidentiality, Availability, Integrity and Non-Repudiation. This framework will work on all the categories of Cloud i.e. Public, Private and Hybrid Cloud and proposes an algorithm to select the correct category of cloud to put a data on to it.

Index Terms— **Cloud Security, Hash Function, Encryption, Indexing, Virtualization.**

I. Introduction

Cloud is simply a distributed network deployed over internet to provide various services, which primarily refers to the storage of the data and files to an offsite location which is owned by a third party which means that user saving its data to another's remote database which is controlled or accessed by user with the help of internet. Cloud can be used to only access files for information which is to gain knowledge and different purposes, i.e., other than file owner so it is necessary to make the data secure according to need of the owner. Basically there are three components of the cloud:

1. *Cloud Service Provider (CSP):* It is the entity which controls and manages the Cloud Storage Server (CSS). It manages the security and various computational aspects of the cloud to manage the client's data.
2. *Client/Owner*: It is the entity which relies on the CSP and stores a large amount of data and uses their resources for their work. It is either a individual or a organization.
3. *User:* It is the unit which is registered under owner and have different access over data.

Cloud ensures the data's security and maintenance, so the security is a major element in a cloud computing infrastructure to ensure the authorised user can only able to access the data and also to protect the data from many type of attack [1, 2]. So according to various security concerns the cloud infrastructure changes a lot and come out to be conclusion of two main concerns

1. External attacker (an unauthorised person)
2. Cloud Service Provider

So there are four major aspects of security which is to be laid out and has to be considered:

1. Confidentiality
2. Availability
3. Integrity
4. Non-Repudiation

The proposed model has focused on the above aspects and has been structured by bringing various methods and techniques to achieve complete secure infrastructure to gain trust among the cloud users. This combination of diverse methods is very much assuring that the data would be secure in cloud. The model uses encryption as its main protection technique to achieve confidentiality and by combining the indexing, classification and hash function it is able to achieve availability, integrity and because of hash function non-repudiation also.

II. Proposed model

Proposed framework is designed to achieve complete security for throughout process of cloud storage. Framework is divided into two phases as explained below:

A. Phase 1(Storage on cloud): This phase deals with the mechanism and methods at time of storage on the cloud can be explained by following sub sections:

1. Classification: As cloud is classified into three sections (Private Cloud, Public Cloud and Hybrid Cloud) it is an important task to classify the data so that it should be stored at right place. This can be achieved by the considering the basic three aspects of cryptography: Confidentiality (C), Availability (A) and Integrity (I). These values can be classified by user on the scale of 5, i.e., {0, 1, 2, 3, 4, 5}, according to their requirement and then the sensitivity(S) of data would be calculated, which decide the classification of the data (Fig 1) by the help of the algorithm (Algo 1).

In the algorithm the section 1 refers to the Owner's Limited Access, section 2 refers to Private and section 3 refers to Public sections of cloud (Fig 1).

Ankit Sharma is M.Tech., Dept. of CSE, Lovely Professional University Phagwara, Jalandhar, India; e-mail:erankitsharma1991@gmail.com

Shashank Guta is M.Tech., Dept. of CSE, Lovely Professional University Phagwara, Jalandhar, India; e-mail:coolshashank22@rediffmail.com

Deep Mann is Asst. Prof., Dept. of CSE, Lovely Professional University Phagwara, Jalandhar, India; e-mail:er.deepmann@gmail.com

Shakil Akhtar is Engineer IV Software Engineer, Cisco, Bangalore, India; e-mail:Shakilsoz17ster@gmail.com

```
Algo 1:
    Inputs: D [ ], D array consist of data
            C [ ], Confidentiality level of data
            A [ ], Availability level of data
            I [ ], Integrity level of data
    Output: Categorized Data for corresponding
    section
1)  For i= 1 to n   //n are number of files
    D [I] =Data / file;
    C[i] =Confidentiality at $i_{th}$ level;
    I[i] =Integrity at $i_{th}$ level;
    A[i] =Availability at $i_{th}$ level;
    //Calculate
    $S[i] =(C[i] + (1/A[i])*5+I[i])/2$
    /*Security is directly proportional to
    confidentiality and integrity and inversely
    proportional to availability*/

2)  For i= 1 to n
    If $S[i] < 2$
    Sec[i] = 3
    If $S[i] \geq 2$ && $S[i] <4$
    Sec[i] = 2
    If $S[i] \geq 4$
    Sec[i] = 1
    /*Sec [ ] represent section allotted to the
    corresponding data*/
```

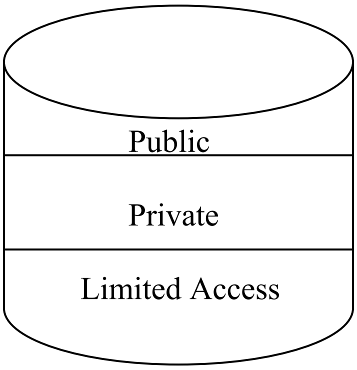

Fig 1. Data segregated into three sections—Sec[3] [Public],Sec[2] [Private],Sec[1] [Owner].

2. *Indexing and Encryption of Data:* Indexing is very important for cloud as we save the data encrypted and in remote sited these indexes would help to search the data from the pool of data.

So after successful allotment of data it is necessary to build the index of the data which can be achieved by an Index Builder and after then we should encrypt our data the whole process is shown in Fig 2.

The encryption technique suggested is ASPE [3] as to overcome the Method of Formal Coding Side Channel Attack (MFCSCA) [4] which is using widely for attacking encryption techniques.

3. *Hash Function:* There are number of Secure Hash Algorithms (SHA) which can be used for providing the Integrity and Non-Repudiation to the user. So it is considered in framework (Fig 3). It is used to check whether the file is tempered or not in the mean-time from storage to retrieval.

4. *Token Generation:* After file is saved to the cloud a token is generated to increase the authentication of the file if it is in lower sections of the file, i.e., Private and Limited Access of the Cloud. This token is used before the downloading of the file.

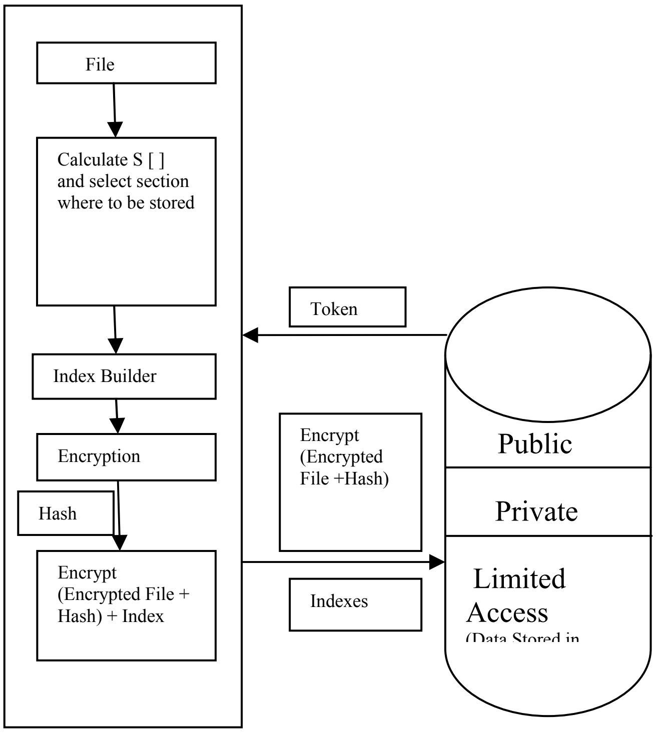
File
Calculate S [ ] and select section where to be stored
Token
Index Builder
Encryption
Hash
Encrypt (Encrypted File + Hash) + Index
Encrypt (Encrypted File +Hash)
Indexes
Public
Private
Limited Access
(Data Stored in

Fig 2. Data Storage from Owner to Cloud

5.

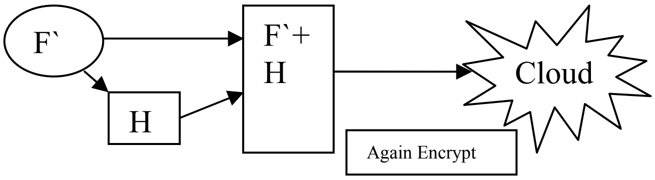

Fig 3. Hash Generation and Sending over Cloud

B. Phase 2 (Retrieval of Data from Cloud): After the secure storage of data work is not over it is important to make equally secure mechanism at the time of retrieval of data.

Firstly, a user has to be enrolled in the client's database (Fig 4), i.e., has proper User Id and password but that is not enough for the retrieval of a data, user would have the specified token assigned for that data to have access(for the lower sections) (Fig 4). If a user would have these two then he can download the file but yet the file is in encrypted form so he has to enter the key to decrypt it and then hash function would match to check the Integrity and non-repudiation of the data (Fig 6). Steps for retrieval are as follows:

1) If the file is at upper level, the user requires the specified User Id and Password assigned by the client/ organization.

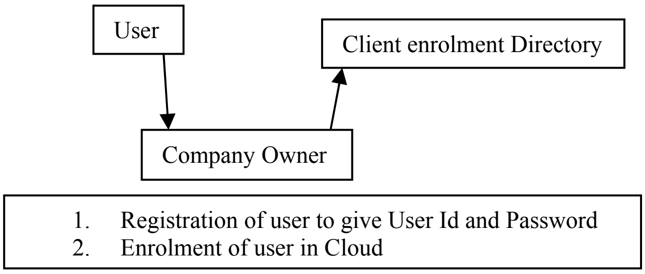
User
Client enrolment Directory
Company Owner
1. Registration of user to give User Id and Password
2. Enrolment of user in Cloud

Fig 4. Enrolment of user in cloud by Owner

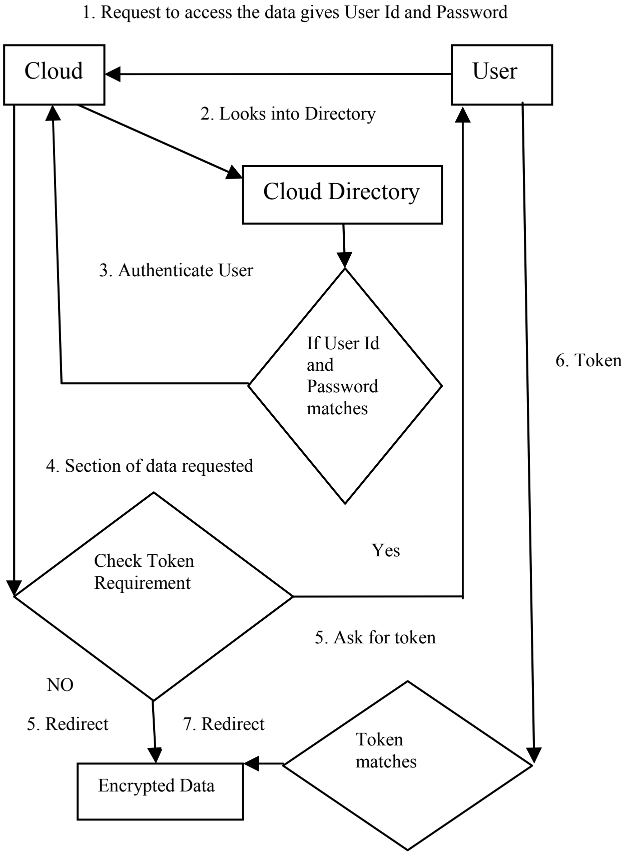

Fig 5. Access request

2) If the file is at lower levels, the user requires the token of the file with the User Id and Password (Fig 5).

After the authentication/ Access request (Fig 5) is granted the user has to follow following steps:

1) User has to decrypt the file.
2) Check hash to verify integrity and non-repudiation.
3) Again decrypt to access the file.

The double encryption ensures the confidentiality and hash function would check its integrity and non-repudiation.

III. Conclusion

Proposed method helps to secure the data and ensures the integrity, authentication and non-repudiation of data. Proposed method has introduced a different section which is able to provide different security aspects through owner to cloud and cloud to user. Even if somebody able to fetch the data it would be in double encrypted form so fetching of original data would be very difficult. It also provides availability by suppressing many issues like tempering of data, data leakage, stoping unauthorised access etc. So, the proposed model helps in ensuring the complete security to enhance reliability.

The future work is to implement the proposed model in the real time scenario and to compare it with other models.

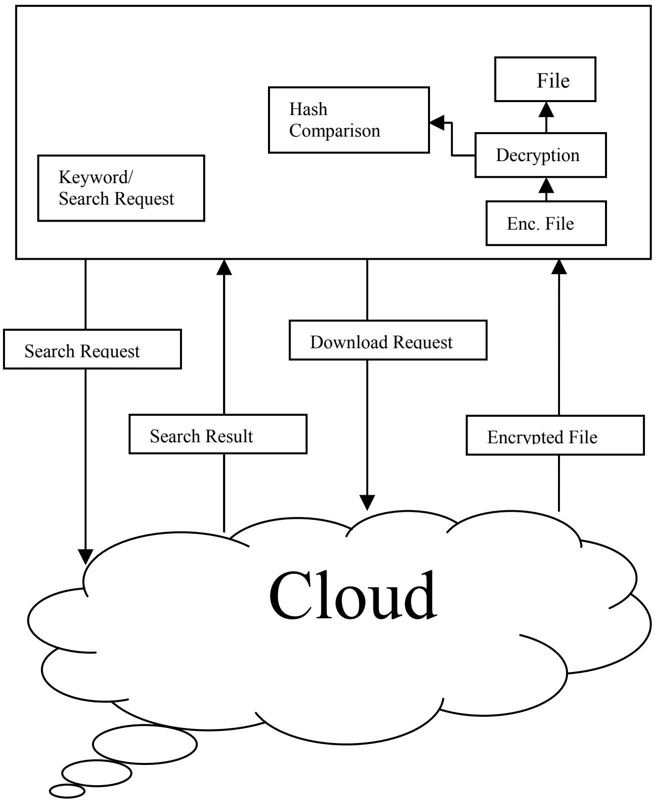

Fig 6. File Retrieval process

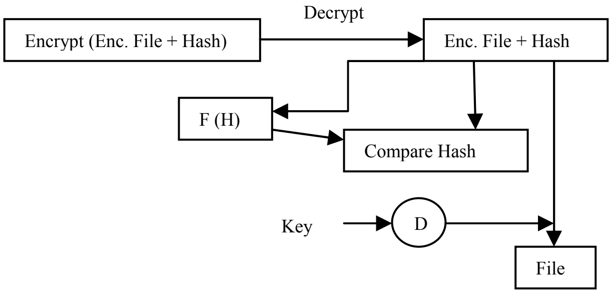

Fig 7. Hash Comparison

References

[1] Daniel EM, Wilson HN. The role of dynamic capabilities in e-business transforma- tion. European Journal of Information Systems 2003;4(12):282–96.
[2] Dikaiakos MD, Katsaros D, Pallis G, Vakali A, Mehra P. Cloud computing. IEEE Internet Computing 2009;12(5):10–3.
[3] Sharma Ankit, Gupta Shashank, Rathode S.K.. Proposal for Portable Approach in Advanced Encryption Standard. International Journal of Computer Science(0975-8887) Volume 69-No. 28 May 2013.
[4] Changyong Peng, Chuangying Zhu, Yuefei Zhu, Fei Kang. Improved side channel attack on the block cipher NOEKEON.
[5] Bowers KD, Juels A, Oprea A. Proofs of retrievability: theory and implementation, Cryptology e-Print Archive. Report 2008/175; 2008a.
[6] Bowers KD, Juels A, Oprea A. HAIL: a high-availability and integrity layer for cloud storage, Cryptology e-Print Archive. Report 2008/489, 2008b.
[7] Cachin C, Micali S, Stadler M. Computationally private information retrieval with polylogarithmic communication, LNCS Springer Verlag, Advances in Cryptol- ogy- EUROCRYPT'99, 1592, p. 402–414, 1999.
[8] Chor B, Gilboa N, Naor M. Private information retrieval by keywords. Report 98-03. Theory of Cryptography Library, 1998.

[9] Chor B, Goldreich O, Kushilevitz E, Sudan M. Private information retrieval, In Proceedings of the 36th annual symposium on foundations of computer science, IEEE, p. 41–51, 1995.

[10] Popa RA, lorch JR, Molnar D, Wang HJ, Zhuang L , Enabling security in cloud storage SLAs with cloudproof. Technical report. Microsoft Research May 2010.

[11] Shacham H, Waters B. Compact Proofs of Retrievability, Proceedings of Asiacrypt '08, 5350, p. 90–107, 2008.

[12] Sood SK, Sarje AK, Singh K. A secure dynamic identity based authentication protocol for multi-server architecture. Journal of Network and Computer Applications 2011;34(2):609–18.

[13] Wang C, Cao N, Li J, Ren K, Lou W. Secure ranked keyword search over encrypted cloud data. Journal of the ACM 2010;43(3):431–73.

[14] Wang C, Wang Q, Ren K, Lou W. Ensuring data storage security in cloud computing, quality of service, 2009, IWQoS IEEE 17th international workshop, p. 1–9, 2009.