IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. VIII (Sep – Oct. 2014), PP 17-23
www.iosrjournals.org

Privacy and Security in Data Storage Using Two Layer Encryption and MAC Verification

Ashly.k.Achenkunju.
(Dept. of Computer Science and Engineering, Mahatma Gandhi University,Kerala, India)

Abstract: *For the privacy and security of data stored in data storage a new Two Layer Encryption (TLE) approach is developed. This technique performs an encryption at two layers based on some ACP(Access Control Policies)on the data owner as well as on the datastorage.The data owner and the data storage utilizes a key management scheme with the help of a key generating algorithmABGKM (Attribute Based Group Key Management)whereby the actual keys do not need to be distributed by the users. The single layer encryption approach using keyword search has some drawbacks such as the privacy of the identity attributes of the users is not taken into account so that the data storage can learn some information about the users and the organization. The random keyword search request also cause loss of information and degrade the privacy of encrypted data. This thesis of two layer encryption allows more secure and private way to handle data updates, user dynamics and policy changes. If there is a change in user dynamics or policy the outer layer of encryption needs to be updated. Since the outer layer encryption is done at the data storage, no transmission of data required between the data owner and data storage. The user who satisfies the access control policies should be able to decrypt the keys twice in order to access the data makes the system more secure and private. Hence my propped thesis has a newly added advantage of two layer encryption using Attribute Based Group Key management (ABGKM) provides a strong secure layer for data storage in servers.*

Keywords: *TLE, PrivacyPresrving, Security, Access Control, ABGKM*

I. Introduction

Now days the most discussing factor in technology is the privacy and security of data. The new technique of this thesis gives a great relief of the burden for storage management. The data owners and the data storage are not in the same trusted domain may put the outsourced unencrypted data at risk. The information in data storage may loss due to some unauthorized access and cause overhead to the dataowner.Although there is some existing methods for resolving this issue, they are not at all satisfied and still there is a need to provide more privacy and security to the data storage. The current systems are like the sensitive data is encrypted before outsourcing the data for privacy and unauthorized access[5].When the large amount of users are searched over the encrypted data the data storage have to go through every restricted files. This explores the security and privacy of datastoarge files. Here my thesis proposing a new scheme for the enhancement of the current existing systems.

The new technique is a dual layer/Two Layer Encryption (TLE) which gives the data storage more security and privacy as the data owners cannot risk their unencrypted outsourced data so as the data storage. The data storage may fail to keep up the integrity of the storage data due to hacking or entry of unauthorized entities. While searching the data in the data storage the attackers prefer the keyword [5] which is not secured properly. The existing technique resolves the optimization complexities in ranked keyword search and its effective utilization of remotely stored encrypted data. But it limits the further optimizations of the search results by preventing server to interact with users to maintain the integrity of actual owner’s keyword and the data associated with it. The aim is to define a framework which enhances the accuracy of the ranked keyword search, which does not affect the data integrity. The data owner performs a coarse grained encryption over the data in order to assure the confidentiality of the data from the storage. Then the data storage performs fine grained encryption over the encrypted data provided by the data owner based on the ACPs provided by the data owner. The new technique overcomes the disadvantage of the security of ranked keywords in the existing system. When the user in the existing system uses keyword randomly in the storage area there may be considerable loss of information and only a single layer encryption is done there that is at the owner side. So there may be a chance of attackers where they can easily decrypt the data. Since my technique is done at two layers of encryption the changes are applied at the outer layer only ,the data should be secure at the inner layer. Using Attribute Based Group Key Management scheme keys are generated and the keys thus generating should not exchange their keys with the owner and the data storage. Hence our system gives more security to the existing system. Encryption of the data is the method to protect the data from malicious and unauthorized users, encryption of the documents can be more than one layer, many layer of the encryption enhance the security of the content For the encryption and decryption of documents keys are used Same key is used in symmetric key approach for encryption and decryption but in asymmetric approach different keys are used to encrypt and decrypt the documents. In symmetric key approach single/one key is used but two keys are used in asymmetric key approach. Here ABGKM (Attribute Based Group Key Management) is used for the generation of keys and by using these keys the secrecy of information is maintained. The AES encryption is used since it provides more security.

The existing scheme provides only single layer of encryption which has some disadvantages such as when users randomly searching there may be loss of information and it is easy for hacking the data. The traditional approach (figure1) is retrieving the files from the server based on some ranking techniques.

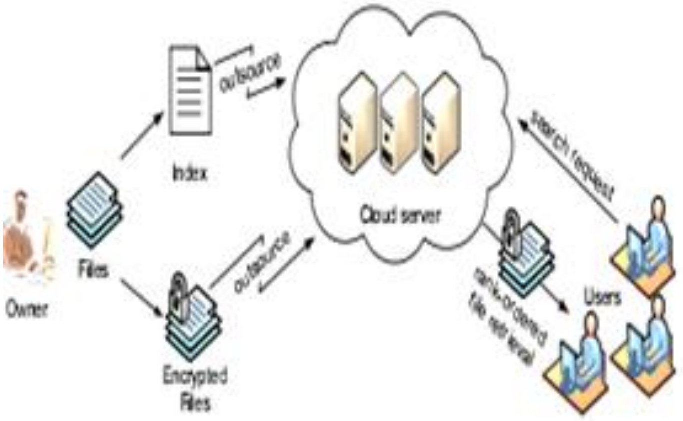


Figure.1. Traditional Approach

In this approach the files are encrypted only by the owners and inverted array indexing techniques is used to provide the searchable encryption of files. The existing scheme uses RSA algorithm for encryption and key generation algorithm for key management. In my proposed schema dual layer encryption is used that is the encryption performs at the two layers the one is by the owner and the other layer is by the cloud server. Since the existing approach is based on some ranking schema by keyword search the user may randomly search the keyword for searching files. This will cause overload to the data owner and thereby the security of data is lost. My new approach of two layer encryption added so many advantages in the existing approaches. The ranking technique of keyword search may cause loss of data during users' continuous intervention in the web. Here comes the importance of our proposed system. The dual layer encryption provides the data more secure at the server level and at the owner level. The AES encryption adds security with the help of ABGKM key generation.

II. Related Work

2.1 Searchable Encryption

To securely search over encrypted data, searchable encryption techniques have been developed by Song and Wagner et al. [1].Searchable encryption schemes usually build up an index for each keyword of interest and associate the index with the files that contain the keyword. By integrating the keywords within the index information, effective keyword search can be realized while both file content and keyword privacy are well-preserved.

Although allowing for performing searches securely and effectively, the existing searchable encryption techniques do not suit for cloud server scenario since they support only exact keyword search. behavior and happen very frequently. As common practice, users may search and retrieve the data of their respective interests using any keywords they might come up with. It is quite common that users' searching input might not exactly match those pre-set keywords. Disadvantage: Searching based on exact keyword match would return unnecessary failures for more making the searching system ineffective with low usability.

2.2 Prefile index scheme for searching

The above limitations are addressed by the works of GohChang,Mitzenmacher et al[2].who propose constructions that associate an \index" to each document in a collection. As a result, the server has to search each of these indexes, and the amount of work required for a query is proportional to the number of documents in the collection. Goh introduces a notion of security for indexes and pseudo-random functions. Chang and

Mitzenmacher achieve a notion of security similar to except that it also tries to guarantee that the trapdoors not leak any information about the words being queried.DisdvantageThe security efficiency of encrypted and unencrypted data is not satisfies since the users query is revealed before a request to the server.

2.3 Fuzzy Keyword search

N.Cao,C.Wang et l[4] investigated the fuzzy keyword search problem in the scenario of a semi-honest-but-curious server, which may execute only a fraction of the search and return part of the searching result honestly. We proposed anew efficient verifiable fuzzy keyword search scheme, which not only supports fuzzy keyword search over encrypted data, but also enjoys the verifiability of the searching result. Though rigorous security and efficiency analysis, we showed that our method is secure and privacy-preserving, while correctly realizing the verifiable fuzzy keyword search.

Disadvantage
It consumes large amount of data storage space and supports only Boolean search.

2.4 Ranked Keyword Search

The problems of the existing systems are avoided with a new concept of ranking schema by Cong Wang [5] of "secure ranked keyword search over encrypted cloud data". Ranked search greatly enhances system usability by enabling search result relevance ranking instead of sending undifferentiated results, and further ensures the file retrieval accuracy. Specifically, we explore the statistical measure approach, i.e., relevance score, from information retrieval to build a secure searchable index, and develop a one-to-many order-preserving mapping technique to properly protect those sensitive score information. The resulting design is able to facilitate efficient server-side ranking without losing keyword privacy.

Disadvantage
1. Keyword search cause loss if information and privacy of data is not as much secured also hackers can easily attack information.
My thesis enhance the security of ranking techniques by providing dual layer encryption which overcomes the security problems of single encryption.

III. Proposed Scheme

My thesis examines the latest scheme of adding security to the existing encryption technique of ranking keyword search by dual layer encryption.

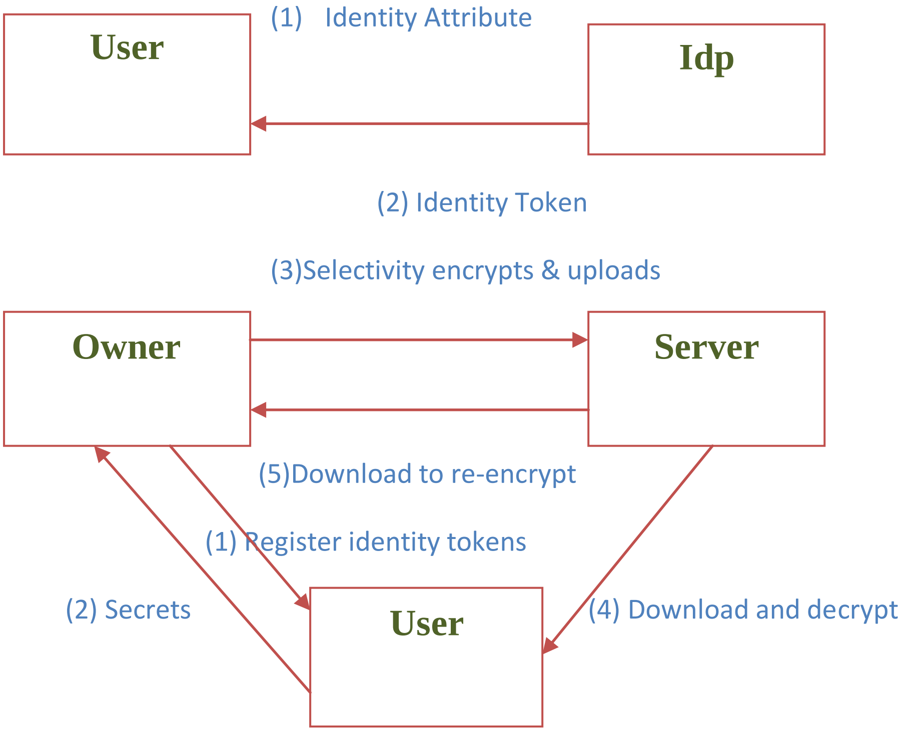


Figure. 2. Single Layer Encryption

A fine grained encryption added at the cloud server enables the system more secure and effective.My proposed architecture is divided into three parts

1. Owner2.User 3.Server

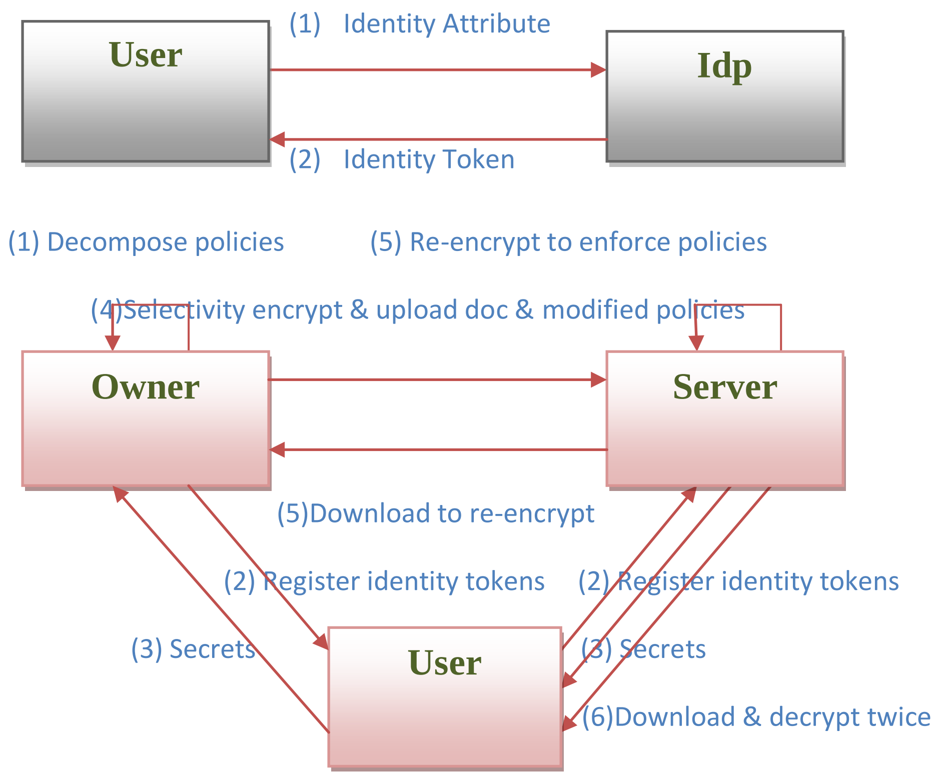

User
Idp
(1) Identity Attribute
(2) Identity Token
(1) Decompose policies
(5) Re-encrypt to enforce policies
(4)Selectivity encrypt & upload doc & modified policies
Owner
Server
(5)Download to re-encrypt
(2) Register identity tokens
(2) Register identity tokens
(3) Secrets
User
(3) Secrets
(6)Download & decrypt twice

Figure. 3. New Architecture

The proposed method(figure 3) is the dual encryption which means the data or information has two layers of encryption. In my scheme the owner will encrypt the data once and later the cloud server encrypts the data for secure storage of data.

The encryption and decryption is performing with the help of a keys generated by ABGKM approach. The encryption technique here used is AES .The outer layer encryption will be decrypted by the cloud and inner layer is decrypted by the user with the help of certainACP's (Access Control Policies).

The existing system of secure and efficient ranked keyword search over data based on some ranking techniques enhance the system usability and enables the system usability by returning the matching files based on the keyword frequency which guarantees the keyword privacy but the security is not satisfied in their work even though the searching is on ranking order. Inverted array index is used here for indexing the files. The users can get more secured data and they can search single and full documents.

Single layer of encryption is done at the existing system. Here comes the latest scheme of "dual layer "to provide the data's more secure and efficient.

My proposed system evaluates the latest advantage of security in privacy preserving of data in cloud servers.

The proposed architecture can be described as

1. Identity token issuance
2. Identity token registration
3. Data encryption and Uploading
4. Data downloading and Decryption
5. Encryption evolution Management

The proposed architecture is gone through these phases. The elaborated description is below.

1. Identity token issuance

When a new user is registered the IDPs provided identity token to the users based on their attributes.

2. Identity token registration

The user should register their identity tokens in order to obtain secrets from the server side as well as the user should register their identity tokens with owner to obtain secrets based on its access control policies.

3. Data encryption and Uploading

The owner first encrypts the data based on some access control policies in order to hide the content from the cloud server and then uploads them along with the public information generated by ABGKM Key generation algorithm. The cloud server in turn encrypts the data based on the keys generated using its own ABGKM Key Generation algorithm.

4. Data downloading and decryption

Users download encrypted data from the Server and have to decrypt twice to access the data. The user gets two keys from the owner and the server if it satisfies the access control policies applied to the data item .

5. Encryption Evolution Management

By the time if access control policies or user credentials changes or already encrypted data may go through further updates the data already encrypted should reencrypt with another key .As the cloud server performs the access control enforcing encryption it simply reencrypts the data.

The functionalities performed by my proposed architecture is

1. Owner: -When a file is uploaded the owner will encrypt the file based on the owner's access control policies in order to hide the data from the cloud server. With the help of AES encryption and ABGKM key generation algorithm the file /data is encrypted. The cloud server in turn encrypts the data based on the keys generated using its own ABGKM Key Generation algorithm.

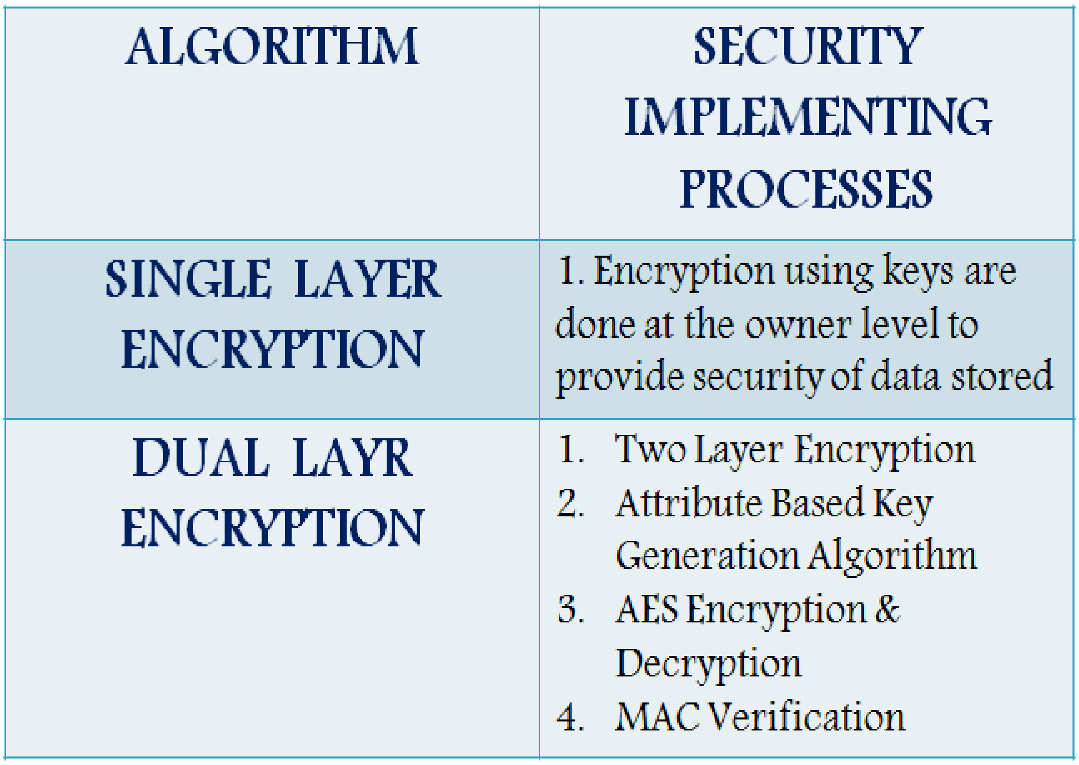
2. User:-When a user requests for a file, if it is a registered user then server and the owner give their secret keys and the user download the file by decrypting the keys twice.

3. Server:-The encrypted data from the user is encrypted with certain access control policies and the key generated using its own ABGKM key generation Algorithm. When the user requests the secret key is passed if it is a registered user. Note that the secret keys of the owner and the cloud server do not know each other.

The ABGKM makes sure that the users who satisfy the access policies can derive the corresponding keys. A user can decrypt the data item only if he satisfies the two parts of the access control policies. At the end of the algorithm neither the owner nor the cloud server never know whether the user met his need. Hence my thesis provide a high security to the data items and reduce the burden of the owner.

IV. Security Analysis

The security of dual layer encryption is as strong as possible compare to the existing systems. The server should not learn the plain text of either the data files or the searched keywords. The existing schema is based on ranked keyword search may cause loss of information or hackers can easily attack the data since the file/data retrieval takes place on the web.



ALGORITHM	SECURITY IMPLEMENTING PROCESSES
SINGLE LAYER ENCRYPTION	1. Encryption using keys are done at the owner level to provide security of data stored
DUAL LAYR ENCRYPTION	1. Two Layer Encryption 2. Attribute Based Key Generation Algorithm 3. AES Encryption & Decryption 4. MAC Verification

My thesis added a security as well as reduce the overhead of data owner since the layers of encryption is performed at two levels .The users frequently interact in web for keyword search may sustain to loss the privacy of the data can be overcome with the help of my thesis. The privacy of the data item is maintained by the dual layer encryption without knowing the secrets of data owner and server each other. Hence the security of the system is increased. The dual layer encryption added the advantage such that if the policy or user dynamics changes only the outer layer of encryption is needed to update. Since it is performed at the server there is no need to transmit the data between them. Hence due to these reasons my thesis gives the latest advantage for both privacy and security of data items. Moreover it gives a solution for the problem of when users are added or removed in the system.

V. Conclusion

The current approaches for outsourcing the data using selective encryption require organizations to manage all keys and encryption need to upload the data to a remote storage. This incur high communication cost as well can degrade the security of the data when the user credentials or access policies changes. The single layer of encryption that is the data is encrypted at the owner side only may subject to the attackers or hackers sometimes. This may cause the loss of our data/information and the privacy of the organization may lose. My thesis of two layer encryption gives a solution to this problem. It performs a dual layer encryption at the inner layer of encryption is performed at the owner level and the outer layer of encryption is performed at the server level. It provides more security than the single layer encryption. The hacker doesn't get the correct data even though our data is hacked. Both the keys should know to decrypt the data correctly. The key management schema by ABGKM algorithm on both the layers not distributed among the owner and the server. MAC verification is done for the users for ensuring more privacy and security. Thus the privacy of the data is maintained. The thesis gives the data storage more secure since the user has to satisfy the access control policies and decrypt twice to get the actual data.

References

[1] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of IEEE Symposium on Security and Privacy'00, 2000.

[2] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. of ACNS'05, 2005.

[3] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Search-able symmetric encryption: improved definitions and efficient constructions," in Proc. of ACM CCS'06, 2006.

[4] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in Proc.of IEEE INFOCOM'10 Mini-Conference, 2010.

[5] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in Proc.of INFOCOM'11, 2011.

[6] AES encryption and decryption-Available: http://en.wikipedia.org/wiki/AES encryption and decryption.

[7] F. Bao, R. Deng, X. Ding, and Y. Yang, "Private query on encrypted data in multi-user settings," in Proc. of ISPEC'08, 2008..

[8] B. Waters, D. Balfanz, G. Durfee, and D. Smetters, "Building an encrypted and searchable audit log," in Proc. of NDSS'04, 2004.

[9] [20] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Service Computing (TSC), to appear.

[10] C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public Auditing for Secure Cloud Storage," IEEE Transactions on Computers (TC), to appear.