An Authentication of Secured Stegnography Using Trapdoor Keys

Ms. T.Jayanthi[1], A. Ram Sravan[2], A. Sharath Kumar Reddy[3]
[1]Assistant Professor, Dept of CSE
[2, 3]Dept of CSE
[1, 2, 3] Sri Chandrasekhrendra Saraswathi Viswa Mahavidyalaya, Deemed to be University Kanchipuram, Tamil Nadu, India

Abstract- *In the earlier system, however significantly limits the usability of outsourced data due to the difficulty of searching over the encrypted data. In the proposed system, Data owner encrypts the data and index using AES encryption sends to cloud server. Also data owner defines access policy for each uploaded file. Server generates a trapdoor of keyword of interest using user's private key and stored in the cloud server. In the modification process, during the registration, every user will generate gets public key & private key. Data owner generates set of trapdoor keys and ABE key which are mailed to the user. 3 -4 Trapdoor keys are generated and everyone is a pair of keys. When server generates 1 key user has to provide another pair of the key which is made steganography with an image & sent to the server. Server de stegno the image and fetches the other pair of the trapdoor key and verifies for authentication. After verification server verifies the access policy for data access through ABE.*

Keywords- Cloud computing, Trapdoor keys, ABE key, Protection, Cryptography, attribute-based keyword search, fine-grained owner-enforced search authorization, multi-user search and verifiable search

I. INTRODUCTION

CLOUD computing has emerged as a new enterprise IT architecture. Many companies are moving their applications and databases into the cloud and start to enjoy many unparalleled advantages brought by cloud computing, such as on-demand computing resource configuration, ubiquitous and flexible access, considerable capital expenditure savings, etc. However, privacy concern has remained a primary barrier preventing the adoption of cloud computing by a broader range of users/applications. When sensitive data are outsourced to the cloud, data owners naturally become concerned with the privacy of their data in the cloud and beyond. Encryption-before-outsourcing has been regarded as a fundamental means of protecting user data privacy against the cloud server (CS). However, how the encrypted data can be effectively utilized then becomes another new challenge. Significant attention has been given and much effort has been made to address this issue, from secure search over encrypted data, secure function evaluation, to fully homomorphic encryption systems that provide generic solution to the problem in theory but are still too far from being practical due to the extremely high complexity. This paper focuses on the problem of search over encrypted data, which is an important enabling technique for the encryption-before-outsourcing privacy protection paradigm in cloud computing, or in general in any networked information system where servers are not fully trusted. Much work has been done, with majority focusing on the single-contributor scenario, i.e., the dataset to be searched is encrypted and managed by a single entity, which we call owner or contributor in this paper. Under this setting, to enable search over encrypted data, the owner has to either share the secret key with authorized users or stay online to generate the search trapdoors, i.e., the "encrypted" form of keywords to be searched, for the users upon request.

II. RELATED WORK

Encrypted data search has been studied extensively designed the first searchable encryption scheme to enable a full text search over encrypted files. Since this seminal work, many secure search schemes have been proposed to boost the efficiency and enrich the search functionalities based on either secret key cryptography (SKC) or public-key cryptography (PKC). An efficient single keyword encrypted data search scheme by adopting inverted index structure. The authors in designed a dynamic version of with the ability to add and delete files efficiently. To enrich search functionalities proposed the first privacy-preserving multi-keyword ranked search scheme over encrypted cloud data using "coordinate matching" similarity measure. Later on a secure multi-keyword text search scheme in the cloud enjoying more accurate search result by "cosine similarity measure" in the vector space model and practically efficient search process using a tree based secure index structure. Compared with symmetric search techniques, PKC-based search schemes are able to generate more flexible and more expressive search queries. Devised the first PKC-based encrypted data search scheme supporting single keyword query.

III. TECHNIQUES USED

- **Advanced Encryption Standard Algorithm:**

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches

❖ **MODULES**

1. Data Owner or User Registration

In this module we are going to create a User application by which the User is allowed to access the data from the Server. Here first the User want to create an account and then only they are allowed to access the Network. Once the User create an account, they are allowed to login into their account to access the application. Based on the User's request, the Server will respond to the User. All the User details will be stored in the Database of the Server. In this Project, we will design the User Interface Frame to Communicate with the Server.

2. Cloud server Deployment

Cloud Data Service Provider will contain the large amount of data in their Data Storage. Also the Cloud Service provider will maintain the all the User information to authenticate the User when are login into their account. The User information will be stored in the Database of the Cloud Service Provider. Also the Data Server will redirect the User requested job to the Resource Assigning Module to process the User requested Job

3. Encryption private & public key generation

In this module, we can design and implementation of private key and public key generation. User registers the private key and public key. In this module we develop a private key and public key for getting access from the cloud owner, when the cloud users want to access the files like download, then he/she has to get the permission from the cloud owner,the cloud owner will verify the keys.

4. Abe access policy

Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text.A crucial security aspect of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

5. Generation of trap door keys

Data owner generates set of trapdoor keys like K1 – RK1, K2 – RK2 and ABE key which are mailed to the corresponding user. Three or four types of trapdoor keys are generated and everyone is a pair of keys.

6. Steganography process

Steganography is the art of hiding of a message within another so that hidden message is indistinguishable. The key concept behind steganography is that message to be transmitted is not detectable to casual eye. Text is used as a cover media for hiding data in steganography. In text steganography, message can be hidden by shifting word and line, in open spaces, in word sequence. Properties of a sentence such as number of words, number of characters, number of vowels, position of vowels in a word are also used to hide secret message. The advantage of preferring text steganography over other steganography techniques is its smaller memory requirement and simpler communication. Hiding the sentence into an image which is called as steganography. Trapdoor keys are made steganography with an image and sent to the server.

IV. PROPOSED WORK

Data owner encrypts the data and index using AES encryption sends to cloud server. Also data owner defines access policy for each uploaded file. Server generates a trapdoor of keyword of interest using user's private key and stored in the cloud server.Every user will generate gets public key & private key. Data owner generates set of trapdoor keys and ABE key which are mailed to the user. 3 -4 Trapdoor keys are generated and everyone is a pair of keys. When server generates 1 key user has to provide another pair of the key which is made steganography with an image & sent to the

server. Server de stegno the image and fetches the other pair of the trapdoor key and verifies for authentication. After verification server verifies the access policy for data access through ABE.

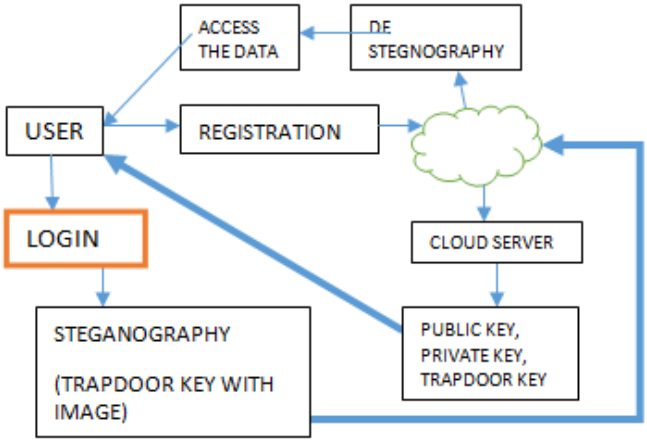


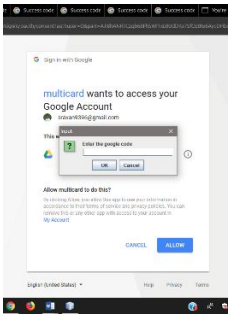
Fig: 1 illustrating the working process of the system

- **Encryption private & public key generation**

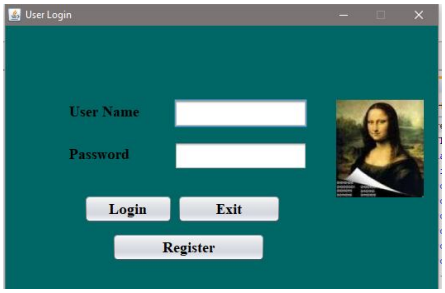
In this module, we can design and implementation of private key and public key generation. User registers the private key and public key. In this module we develop a private key and public key for getting access from the cloud owner, when the cloud users want to access the files like download, then he/she has to get the permission from the cloud owner,the cloud owner will verify the keys**.**

PROGRESS:

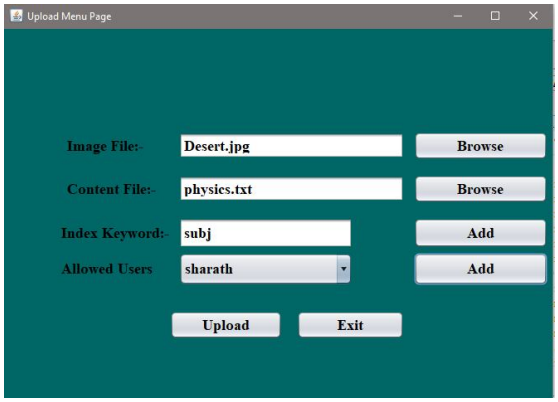
1. Google drive permission



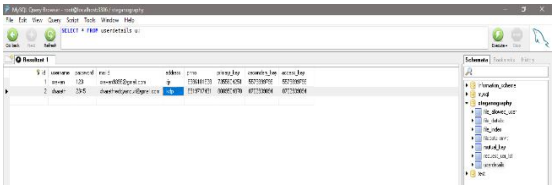
2. Login & Register page



3. Uploading Document



4. Data Base



V. CONCLUSION

In this design the first verifiable attribute-based keyword search scheme in the cloud environment, which enables scalable and fine-grained owner-enforced encrypted data search supporting multiple data owners and data users. Compared with existing public key authorized keyword search scheme, our scheme could achieve system scalability. Different from search scheme with predicate encryption, our scheme enables a flexible authorized keyword search over arbitrarily- structured data. In addition, by using proxy re-encryption and lazy re-encryption techniques, the proposed scheme is better suited to the cloud outsourcing model and enjoys efficient user revocation. On the other hand, we make the whole search process verifiable and data user can be assured of the authenticity of the returned search result. We also formally prove the proposed scheme semantically secure in the selective model.

REFERENCES

[1] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: Attribute-based keyword search with fine-grained owner enforced search authorization in the cloud," in Proc. IEEE Conf. Comput. Commun., 2014, pp. 226–234.

[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE Conf. Comput. Commun, 2010, pp. 1–9.

[3] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[4] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. 14th Int. Conf. Financial CryptographyData Security, 2010, pp. 136–149.

[5] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Security Privacy, 2000, pp. 44–55.

[6] Y. Huang, D. Evans, J. Katz, and L. Malka, "Faster secure twoparty computation using garbled circuits," in Proc. 20th USENIX Conf. Security Symp., 2011, p. 35.

[7] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Stanford, CA, USA, 2009.

[8] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 79–88