

Adaptable Wildcard Searchable Encryption System

Savi P. Ghadge¹, Yogesh A. Patil², Shivani K. Wankhede³, Guided by Ms. Pradnya Kasture⁴

^{1,2,3}Student, Department of Computer Engineering RMD Sinhgad School of Engineering Pune, India

⁴Assistant Professor, Department of Computer Engineering RMD Sinhgad School of Engineering Pune, India

Abstract - Searchable Encryption is a cryptographic technique which allows search of data in an encrypted format. This technique provides user data confidentiality insurance for public cloud storage service as well as allows multiple keyword search over encrypted data. Previously existing systems provide exact or fuzzy keyword search which corrects spelling errors only and their features are limited. In this paper, we propose a system known as adaptable wildcard searchable encryption system which allows multiple keyword search with auto generated wildcards and wildcard keyword queries with additional features. In the proposed framework a proxy server is presented for the recovery of lost data over malicious activities. It accomplishes a high level of security assurance since coordinating outcomes are obscure to the cloud server in the test stage.

Key Words: Searchable Encryption, Multiple keyword search, Auto generated wildcard search, Security assurance.

1. INTRODUCTION

Cloud computing greatly facilitates data providers who want to outsource their data to the cloud without disclosing their sensitive data to external parties and would like users with certain credentials to be able to access the data. This requires data to be stored in encrypted forms with access control policies such that no one except users with attributes (or credentials) of specific forms can decrypt the encrypted data. An encryption technique that meets this requirement is required, where a user's private key is associated with an attribute set, a message is encrypted under an access policy (or access structure) over a set of attributes, and a user can decrypt a cipher text with his/her private key if his/her set of attributes satisfies the access policy associated with this cipher text. However, the standard ABE system fails to achieve secure deduplication, which is a technique to save storage space and network bandwidth by eliminating redundant copies of the encrypted data stored in the cloud. On the other hand, to the best of our knowledge, existing constructions for secure deduplication are not built on attribute-based encryption. Nevertheless, and secure deduplication have been widely applied in cloud computing, it would be desirable to design a cloud storage system possessing both properties.

Attribute-based encryption (ABE) has been widely used in cloud computing where a data provider outsources his/her encrypted data to a cloud service provider, and can share the data with users possessing credentials (or

attributes). However, the standard ABE system does not support secure deduplication, which is crucial for eliminating duplicate copies of identical data in order to save storage space and network bandwidth.

We present an attribute-based storage system with secure deduplication in a hybrid cloud setting, where a private cloud is responsible for duplicate detection and a public cloud manages the storage.

2. LITERATURE SURVEY

Flexible wildcard searchable encryption system by Yang Yang, Ximeng Liu, Members, IEEE, Robert H. Deng, Fellow IEEE, Jian Weng. According to this paper published in 2017, searchable encryption is used to provide data confidentiality and to allow users search over encrypted data with wildcard keyword queries. In this system wildcards need to be defining while uploading a file.

Hidden Policy cipher text-policy attribute based encryption with keyword search against keyword guessing attack by Qui S, Liu J, Shi Y, et al, 2017 states attribute based keyword search and policy.

Fuzzy keyword search over encrypted data in cloud computing by Li J, Wang Q year 2010. Exploited edit distance to measure keywords similarity. It only deals with exact or fuzzy keyword search to correct some spelling errors.

Efficient wildcard search over encrypted data by Hu C, Han L in year 2015 introduced wildcard search over encrypted data but there was no auto generation of wildcard.

3. SYSTEM ANALYSIS

3.1 Existing System:

Fuzzy keyword search introduced in the existing system deal with exact or fuzzy keyword only to correct spelling errors. The edit distance to measure keyword similarity is small. It is useless if the edit distance of query keyword is large. It was impossible to search multiple users' data simultaneously using one trapdoor. It is constructed based on bloom filter. These Bloom filter based wildcard searchable encryption schemes return false results to users with a no negligible probability. Hence it decreases the Security assurance. Flexible wildcard searchable encryption does not generate wildcard automatically. There is no recovery option for the lost data.

3.2 Proposed System:

To save storage space and network bandwidth by eliminating redundant copies of the encrypted data stored in the cloud we propose a cloud storage system with both properties associate attribute-based storage system with secure De-duplication. De-duplication during a hybrid cloud environment, wherever a personal cloud is chargeable for duplicate detection and a public cloud manages the storage planned system compared with the previous information de-duplication systems. As our system support high security and potency, additionally to boot file transfer upload file by specifying period and access policy.

In our system, we check deduplication of content by using tag and upload file in encryption format. Then system will auto generate wildcard of all files and store on cloud. End user can download this file by using a private key sent by the TPA while uploading the file. We propose a proxy server for the recovery of lost data.

4. IMPLEMENTATION

4.1 Data Owner:

Initially the data owner will upload their respective files on cloud with attribute constrained like time, date and access policy. After that the private key get generated automatically which is known only to data owner and copy of that key is get stored at TPA side for future work. Only the data owner having the rights to download the encrypted file by using key which is generated at storing time. If the another user wants to download that file, he/she must know the decryption key, if the key get matched then the user can able to access or download that file successfully.

4.2 Third Party Authorizer:

The role of third party authorizer is to grant excess policy to users except data owner by providing tag and key to download the cloud stored data. TPA also checks for hacked file by sending request to proxy server. By providing file status it give us privacy policy. Data owner can recover the hacked data or file by help of TPA; TPA regenerates the tag and key for recovered data.

4.3 Proxy Server:

The main role of proxy server is to check whether the cloud stored file is get hacked or not. If the data owner requested for stored file status then proxy server get invokes and as per file contained data, the server checks whether the file is get malicious or not, if changes occurred, then it will acknowledged to TPA that file is get hacked and as per data owner request proxy server get recovered all the hacked data.

4.4 Cloud Storage:

Cloud storage is file storage in the cloud (online). Instead of keeping your files on your local hard drive, external hard drive, or flash drive, you can save them online. Cloud Server provides data storage space for the user/data owner to store the data that provides the secured and efficient way of storing the owner's data.

5. SYSTEM ARCHITECTURE

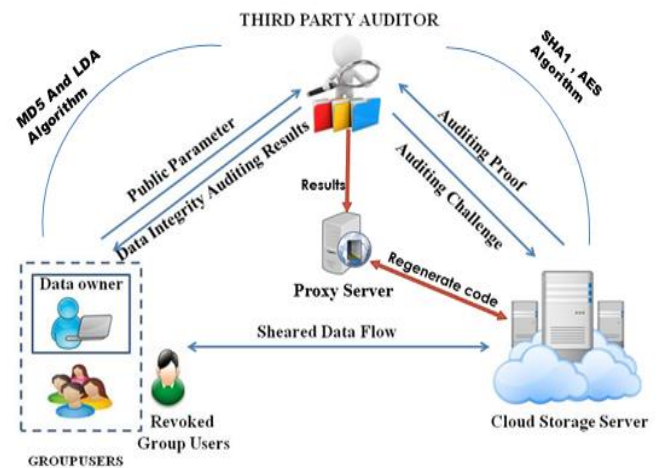
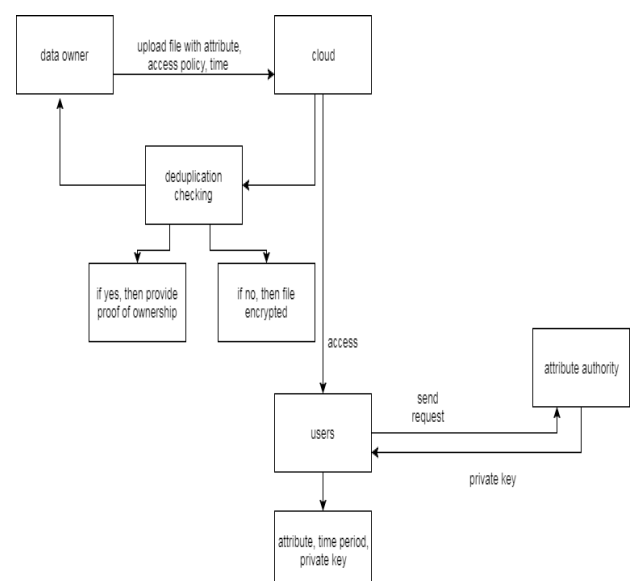


Fig -1: System Architecture

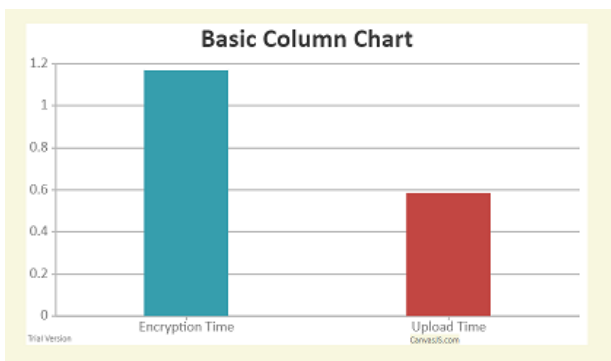
An entity who named as data owner who upload the files with attribute, time, access policy, time, deduplication. The uploaded files store on cloud but before that file get check weather file is original or duplicate. And an user who request for file for downloading the file and to access the file. We used AES algorithm for Encryption and Decryption of data.

6. DATAFLOW DIAGRAM

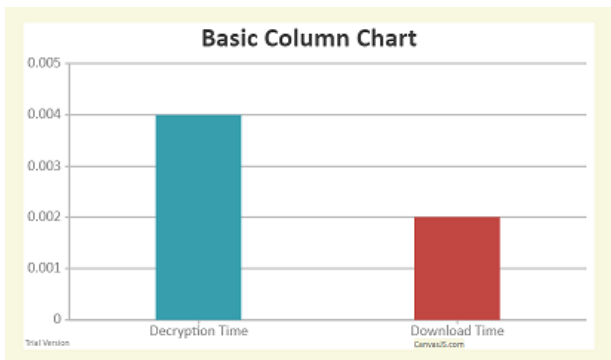


Initially the data owner will upload their respective files on cloud with attribute constrained like time, date and access policy with a tag. After that the stored data will be checked for deduplication, if the uploaded file is original then the file will get encrypted otherwise will give reference to original one which is on cloud. When the user wants to access that files which are stored on cloud, will send request to TPA, after conforming the constrained the TPA will send private key to user to decrypt the file and then user can successfully download the desired file.

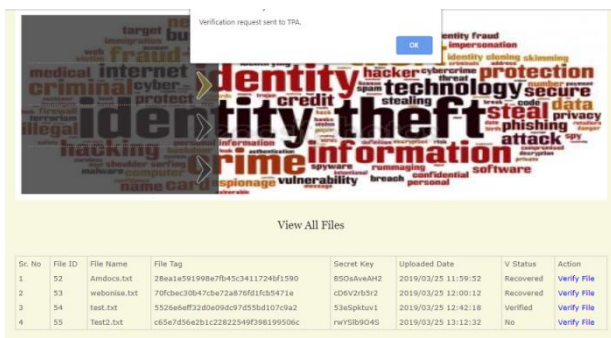
7. SYSTEM UI



Above graph shows the time required to encrypt data while storing on cloud.

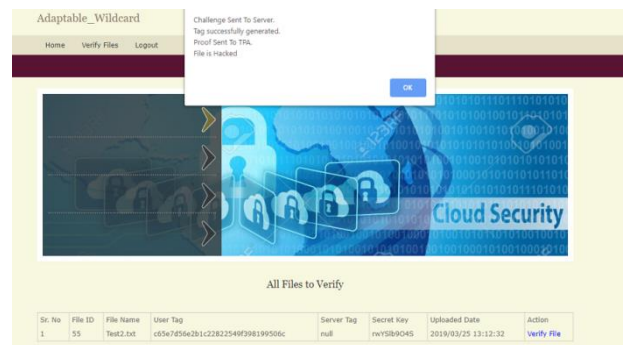


Above graph shows the time required to decrypt data while downloading from cloud.



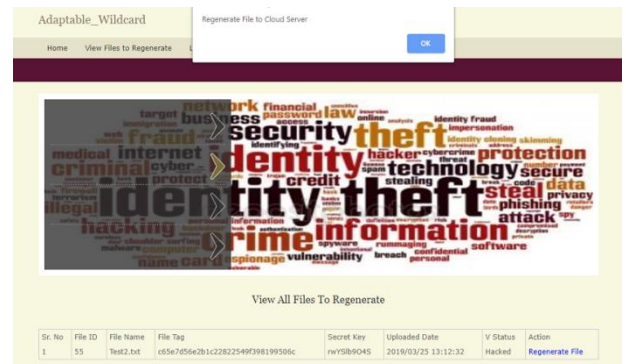
Sr. No	File ID	File Name	File Tag	Secret Key	Uploaded Date	V Status	Action
1	52	Amdocs.txt	28aa1e591998e7b45c34117248f1590	850aAveAH2	2019/03/25 11:59:32	Recovered	Verify File
2	53	webdocs.txt	70f0bc30b47c3e72a876f01f035473a	cd6v2f552	2019/03/25 12:00:12	Recovered	Verify File
3	54	test.txt	553860aff723d0909d07f85b0d1070d2	33a6pkuv1	2019/03/25 12:42:18	Verified	Verify File
4	55	Test2.txt	cd5e7d56e2b1c22822549f398199506c	rwYSB9Q45	2019/03/25 13:12:32	No	Verify File

When data owner wants to check whether the cloud stored file is get hacked or not, request will sent to TPA as per privacy policy.



Sr. No	File ID	File Name	User Tag	Server Tag	Secret Key	Uploaded Date	Action
1	55	Test2.txt	cd5e7d56e2b1c22822549f398199506c	null	rwYSB9Q45	2019/03/25 13:12:32	Verify File

To check any malicious data or any changes occurred in cloud stored data file, whether the cloud stored file is get hacked or not, response will send back to TPA as per privacy policy.



Sr. No	File ID	File Name	File Tag	Secret Key	Uploaded Date	V Status	Action
1	55	Test2.txt	cd5e7d56e2b1c22822549f398199506c	rwYSB9Q45	2019/03/25 13:12:32	Hacked	Regenerate File

If any malicious data or any changes occurred in cloud stored data file, if the cloud stored file is get hacked, regeneration of file tag is carried out by sending request to proxy server by TPA as per privacy policy and hacked data will get recovered successfully.

8. CONCLUSION

Our proposed system provides a new and adaptable wildcard searchable encryption system for secure cloud storage service, which supports flexible wildcard representation, flexible search function and flexible user authorization revocation. By reducing rate of hacked data, system successfully recovered the hacked files to produce security factor to stored data.

9. REFERENCES

[1] Yang Yang, Ximeng Liu, Robert H. Deng, Jian Weng, "Flexible Wildcard Searchable Encryption System", IEEE Transactions on Services Computing, June 2017.

[2] Singh A, Chatterjee K. Cloud security issues and challenges: A survey[J]. Journal of Network and Computer Applications, 2017, 79: 88-115.

- [3] Qiu S, Liu J, Shi Y, et al. Hidden policy ciphertext-policy attribute based encryption with keyword search against keyword guessing attack[J]. Science China Information Sciences, 2017, 60(5): 052105.
- [4] Yang Y, Ma M. Conjunctive Keyword Search With Designated Tester and Timing Enabled Proxy Re-Encryption Function for EHealth Clouds[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(4): 746-759.
- [5] Yang Y. Attribute-based data retrieval with semantic keyword search for e-health cloud[J]. Journal of Cloud Computing, 2015, 4(1): 1.
- [6] Hu C, Han L. Efficient wildcard search over encrypted data[J]. International Journal of Information Security, 2015: 1-9.
- [7] Li J, Chen X. Efficient multi-user keyword search over encrypted data in cloud computing[J]. Computing and Informatics, 2013, 32(4): 723-738.
- [8] Suga T, Nishide T, Sakurai K. Secure keyword search using Bloom filter with specified character positions[C]//International Conference on Provable Security. Springer Berlin Heidelberg, 2012: 235-252.
- [9] Bosch C, Brinkman R, Hartel P, et al. Conjunctive wildcard search over encrypted data[C]//Workshop on Secure Data Management. Springer Berlin Heidelberg, 2011: 114-127.
- [10] Li J, Wang Q, Wang C, et al. Fuzzy keyword search over encrypted data in cloud computing[C]//INFOCOM, 2010 Proceedings IEEE. IEEE, 2010: 1-5
- [11] Boneh D, Di Crescenzo G, Ostrovsky R, et al. Public key encryption with keyword search[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2004: 506-522.