DATA ISOLATION USING FINE-GRAINED ACCESS CONTROL FOR SEARCHABLE ENCRYPTION

SURI.RAVI PG Scholar, Dept of CSE, Quba College of Engineering & Technology, Venkatachalam, AP, India.

D.MURALI Assistant Professor, Dept of CSE, Quba College of Engineering & Technology, Venkatachalam, AP, India.

ABSTRACT

Cloud servers can scan over encrypted data without having to decode it thanks to searchable encryption. A user can view a subset of documents that include the keyword of their choice thanks to single-keyword searchable encryption. For applications where several data owners upload their data and different users can access the data, we provide a single keyword-based searchable encryption strategy in this work. The system makes use of attribute-based encryption to let users access a specific portion of cloud data without disclosing their access credentials to the cloud server..In the random oracle model, the technique is demonstrated to be adaptively secure against chosen-keyword attacks. We put the plan into practice on a Google cloud instance, and its effectiveness was discovered to be useful in real-world applications..

1. INTRODUCTION

Due to the availability of on-demand data and services at lower costs in an effective manner, many firms find that outsourcing data to the public cloud supports an appealing business strategy. To the service provider and service users, however, the security and privacy of data have grown to be major concerns as organisations employ cloud services, particularly public cloud, to achieve their business objectives. When sensitive information is contained in outsourced data, such as in personal health records (PHRs), bid information submitted for a tender, financial records of an individual or organization, and so on, the cloud server or unauthorized users may be able to access the data and/or infer sensitive information..One workable solution to the problem of data privacy and access control is to encrypt the documents prior to outsourcing them to a cloud storage server. Consider the use cases where several data owners upload their encrypted documents to public cloud storage services and various users have access to the documents stored on the cloud storage server. Using a fine-grained access control policy in these applications will enable the desired security control on document access..

An intriguing cryptographic technique called Attribute Based Encryption (ABE)[1] enables data secrecy and owner-enforced fine-grained access control. With an ABE scheme, a data owner can encrypt a message using a set of attribute values (such as an access policy) so that only authorized parties who have the necessary set of attribute values can decrypt the cypher text. A practical necessity for contemporary cloud storage data is the ability to explore databases with encrypted data. Many methods for searching over encrypted data have been introduced in the field of searchable encryption. A receiver may be able to securely and arbitrarily get data from publicly available cloud storage that is of interest to them by using searchable encryption..For instance, a doctor may want to look up all of his patients' records who have been identified as having chronic renal disease and for whom he has been granted access to their medical information, each of which has been encrypted and uploaded by the patient. Single-user searchable symmetric encryption techniques cannot be applied in this situation since the patient must first encrypt his medical records with a secret key before sharing it with the doctor..A data owner, such as a patient, can create a shared secret key or search token from his master secret key and distribute it to the authorized users (in our example, the doctor) for searching over encrypted data. As a result, multi-user searchable symmetric encryption schemes [6–8] are the most effective for requiring searches over encrypted data and enforcing access control policies. Although these schemes can function in a single-sender, multiple-receiver configuration, they are unable to function effectively in a multi-sender, multiple-receiver configuration because each data sender must securely communicate with each data receiver in order to distribute the secret key or search token, incurring a significant communication overhead..The goals of searching across encrypted data and implementing fine-grained access control rules can both be achieved instead by using keyword-based searching over attribute-based encrypted data. In scenarios with several senders and receivers, the ABE scheme performs effectively. Direct communication between the data owner and the data receiver is not necessary. For the purpose of enabling single keyword searches over attribute-based encrypted data, numerous techniques for keyword-based searching over encrypted data have been developed in [9–12]. The Wang et al. approach [9] offers single keyword searches and assigns a portion of the decryption effort to the cloud service provider..The search system in [10] not only allows for searching over encrypted data but also for the verifiability of search results. The plan in [11] offers keyword search verifiability over attribute-based encryption with key policy. In addition to keyword-based search operation over encrypted data, the developers of [12] also addressed the issues of data sharing and keyword updating. The [13] scheme offers a disjunctive multikeyword search option. Dong et al. [14] suggested a plan that uses an online-offline strategy to offer an effective keyword-based searching operation over ABE. Proxy re-encryption (PRE) and a secret sharing scheme (SSS) are both incorporated into the [15] scheme. Nonetheless, all of these schemes have clearly defined access control policies..Protecting user privacy is a crucial criterion in order to maintain the confidentiality of the data and/or the goal of the service requested [2-5]. The attacker can identify the receiver by using the attributes that are revealed by the access policy that is connected to the encryption text in clear form. Due to this worry, the access policy is frequently regarded as confidential information because the cypher text shouldn't make the contents of the cypher text's contents obvious. For instance, in a healthcare setting, an adversary can infer information about the patient's ailment from the access policy of the patient's medical report..As a result, maintaining the privacy of data access is a practical necessity in addition to maintaining the confidentiality of the data, as doing so would allow one to deduce the cypher text's intended use. If an encrypted document's access policy is listed in plain form, the adversary will find it easier to extract the receiver information, and the receiver information can then be used to reveal statistical statistics about the encrypted data. The access policy must be in a hidden form to solve this issue. The hidden access policy protects the confidentiality of the encrypted text's intent and intended readership.

2. PROBLEM STATEMENT

The attacker can identify the receiver by using the attributes that are revealed by the access policy that is connected to the encryption text in clear form. Due to this worry, the access policy is frequently regarded as sensitive information because the encrypted text should not make its contents visible..

For instance, in a healthcare organization, an adversary can infer information about the patient's ailment from the access policy of the patient's medical report. As a result, maintaining the privacy of data access is a practical necessity in addition to data confidentiality because doing so would allow one to deduce the cypher text's intended use..

If an encrypted document's access policy is published in plain form, the adversary will find it easier to extract the receiver information, and the receiver information can then reveal statistical statistics about the encrypted data.

2.1 LIMITIATIONS

In the literature, there are numerous attribute-based, keyword-searchable encryption algorithms. Unfortunately, the crucial issue of receiver anonymity is left unaddressed by these approaches..

3. PROPOSED SYSTEM

We introduce a single keyword-based searchable encryption scheme (PSE) that protects privacy and has granular access control. The proposed PSE approach offers attribute-based encrypted data with hidden access rules and a keyword-based search function. The plan can be used in a situation where there are numerous data owners and recipients..

A trusted authority verifies each user's attributes and gives him a secret key according to the scheme, which allows each user in the system to have a set of attribute values. One of the most important aspects of the PSE scheme is that, after obtaining the secret key, the user can create the search query on his own in the form of a trapdoor by utilising the secret key supplied to him.

3.1 ADVANTAGES

The PSE scheme protects data confidentiality and user access rights privacy. The PSE scheme's search functionality has demonstrated adaptive security against chosen-keyword attacks. Over encrypted documents kept on CSP, the PSE method enables authorized users to obtain a subset of those documents.

4. IMPLEMENATION

4.1 Data Owner

The data owner uploads their data to the cloud server in this module. The data owner encrypts the file and the index name for security reasons before storing them in the cloud. A specific file can be deleted by the data encryptor. Also, he will perform the following procedures and observe the transactions based on the files he uploaded to the cloud. Login and Register Owners, Need cloud to grant enc key access and see resources, enc, browse the file, apply the ABE, and upload All uploaded files can be seen with a digital signature. Go over your files and update the content, Browse your files and delete them, View the security request and grant it.

4.2 Data User

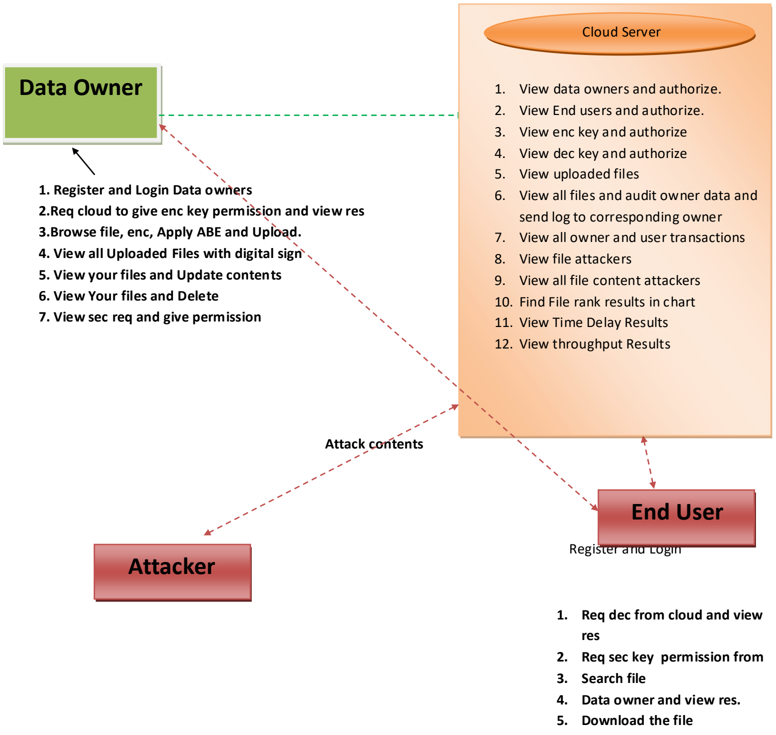
User logs in to this module using user name and password. After logging in, the user requests search control in the cloud, searches for files using the index term, receives a search result score, and downloads the file. The user can view the results of a file search and perform other operations such as requesting a cloud-based dec and viewing the results, requesting sec key authorization from a third party, searching a file, and viewing the results for a certain data owner. Save the file..

4.3 Cloud Server

A cloud is managed by a cloud server to offer data storage services. For sharing with Remote Users, data owners encrypt and store their data files on the cloud. Data consumers download and decrypt the encrypted data files they want from the cloud in order to access the shared data files. The cloud server grants permission to the data owner and user and fulfils user-submitted search queries. The personalised search model and the interest search model are also displayed in this section..may inspect every file attacker and perform the following actions examine data owners and consent, See End users and give permission, View the EC key and approve, Observe the Dec key and approve, View uploaded documents, See all files and audit owner data and send log to associated owner, See each owner- and user-related transaction. look at file attackers, See all attackers of file content, Chart showing file ranking outcomes Look at the Time Delay Results, View results for throughput

5. SYSTEM ARCHITECTURE

Architecture Diagram



Cloud Server:

1. View data owners and authorize.
2. View End users and authorize.
3. View enc key and authorize
4. View dec key and authorize
5. View uploaded files
6. View all files and audit owner data and send log to corresponding owner
7. View all owner and user transactions
8. View file attackers
9. View all file content attackers
10. Find File rank results in chart
11. View Time Delay Results
12. View throughput Results

Data Owner:

1. Register and Login Data owners
2.Req cloud to give enc key permission and view res
3.Browse file, enc, Apply ABE and Upload.
4. View all Uploaded Files with digital sign
5. View your files and Update contents
6. View Your files and Delete
7. View sec req and give permission

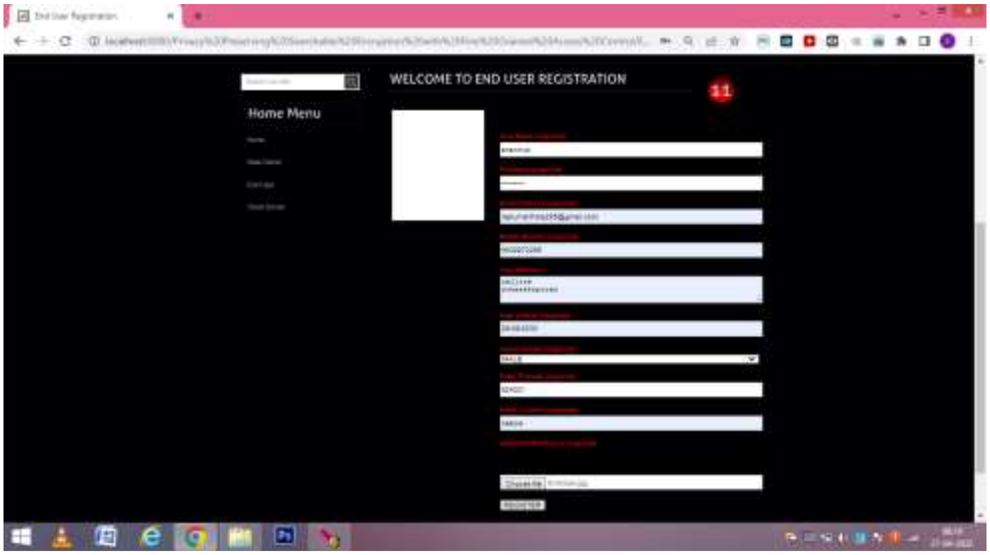
End User:

1. Req dec from cloud and view res
2. Req sec key permission from
3. Search file
4. Data owner and view res.
5. Download the file

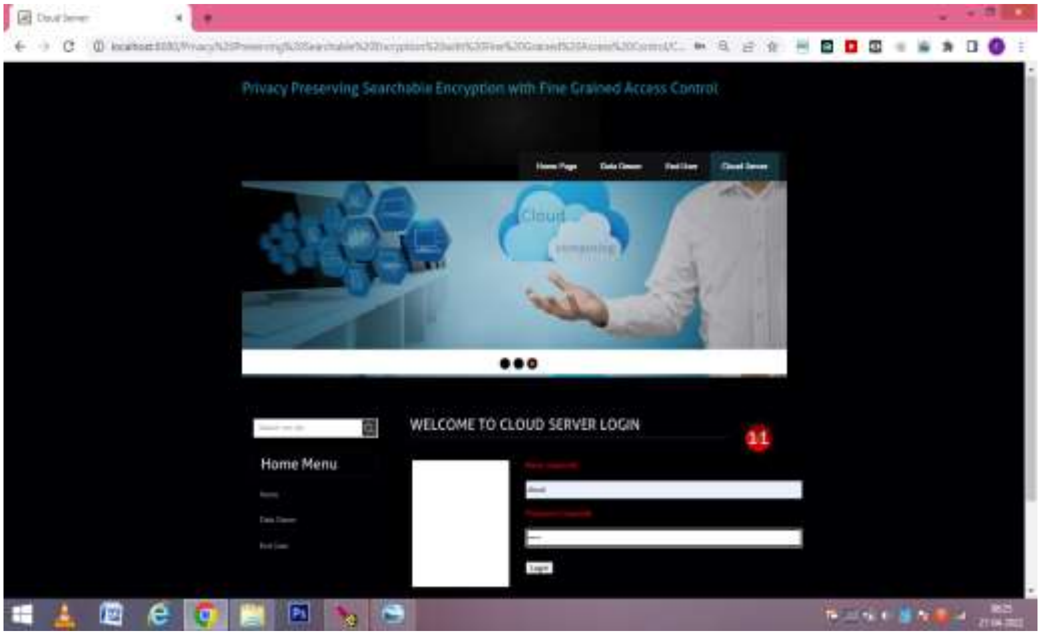
6. SCREEN SHORTS

Privacy Preserving Searchable Encryption with Fine Grained Access Control

WELCOME TO END USER LOGIN

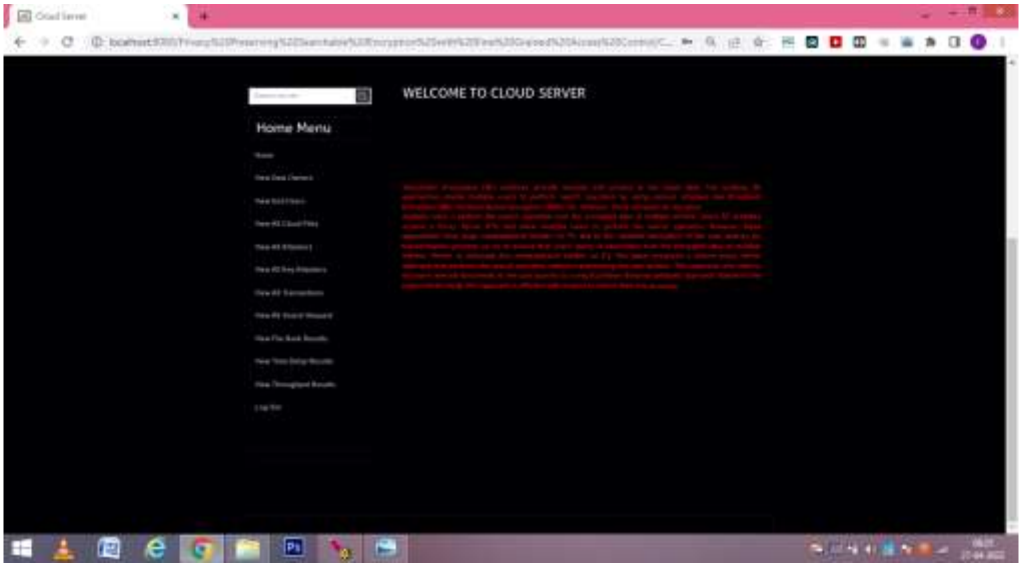


WELCOME TO END USER REGISTRATION



Privacy Preserving Searchable Encryption with Fine Grained Access Control

WELCOME TO CLOUD SERVER LOGIN



7. CONCLUSION

We suggested an attribute-based searchable encryption method that protects privacy. An authorised user can retrieve a subset of documents, over encrypted documents stored on CSP, that satisfy his access privileges and relate to his chosen keyword using the suggested PSE scheme. The PSE scheme protects data confidentiality and user access rights privacy. Under the DBDH assumption in the random oracle model, the search functionality of the PSE scheme is demonstrated to be adaptively safe against chosen-keyword attacks. The PSE system was put into practise on a Google cloud instance, and its effectiveness was found to be useful in real-world applications.

REFERENCES

[1] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the ACM Conference on Computer and Communications Security, pp. 89–98, 2006.

[2] T. Nishide, K. Yoneyama, and K. Ohta. Attribute-based encryption with partially hidden encryptor-specified access structures. In Proceedings of Applied Cryptography and Network Security, LNCS 5037, Springer, pp. 111–129, 2008.

[3] J. Li, K. Ren, B. Zhu, and Z. Wan. Privacy-aware attribute-based encryption with user accountability. In Proceedings of Information Security, LNCS 5735, Springer, pp. 347– 362, 2009.

[4] Y. Zhang, X. Chen, J. Li, D. S. Wong, and H. Li. Anonymous attribute-based encryption supporting efficient decryption test. In Proceedings of the ACM SIGSAC Symposium on Information, Computer and Communications Security, pp. 511–516, 2013.

[5] P. Chaudhari, M. L. Das, and A. Mathuria. On Anonymous Attribute Based Encryption. In Proceedings of the International Conference on Information Systems Security, LNCS 9478, Springer, pp. 378–392, 2015.

[6] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky, Search- able symmetric encryption: improved definitions and efficient constructions. Journal of Computer Security. 19(5), pp. 895–934, 2011.

[7] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M. C. Rou, M. Steiner, Highly-scalable searchable symmetric encryption with support for boolean queries. In Advances in Cryptology-CRYPTO, Springer, pp. 353-373, 2013

[8] S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, M. Steiner. Outsourced symmetric private information retrieval. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, ACM pp. 875-888, 2013.

[9] C. Wang, W. Li, Y. Li, and X. Xu. A ciphertext-policy attribute-based encryption scheme supporting keyword search function. In Proceedings of Cyberspace Safety and Security, LNCS 8300, Springer, pp. 377–386, 2013.

[10] Q. Zheng, X. Shouhuai, and G. Ateniese. VABKS: Verifiable attribute-based keyword search over outsourced encrypted data. In Proceedings of IEEE Conference on Computer Communications (INFOCOM), pp. 522–530,2014.

[11] P. Liu, W. Jianfneg, M. Hua, and N. Haixin. Efficient verifiable public key encryption with keyword search based on KP-ABE. In Proceedings of International Conference on Broadband and Wireless Computing, Communication and Applications, pp. 584–589, 2014.

[12] K. Liang and W. Susilo. Searchable attribute-based mechanism with efficient data sharing for secure cloud storage. In IEEE Transactions on Information Forensics and Security 10(9):1981–1992,2015.

[13] J. Li and L. Zhang. Attribute-based keyword search and data access control in cloud. In Proceedings of International Conference on Computational Intelligence and Security, pp. 382–386, 2014.

[14] Q. Dong, Z. Guan, and Z. Chen. Attribute-based keyword search efficiency enhancement via an online/offline approach. In Proceedings of IEEE International Conference on Parallel and Distributed Systems, pp. 298–305, 2015.

[15] B. Hu, Q. Liu, X. Liu, T. Peng, G. Wang, and J. Wu. DABKS: Dynamic attribute-based keyword search in cloud computing. In Proceedings of IEEE International Conference on Communications, pp. 1–6, 2017.

[16] D. Koo, J. Hur, and H. Yoon. Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage. In Computers & Electrical Engineering, Elsevier, pp.34–46, 2013.

[17] P. Chaudhari and M. L. Das. On the Security of a Searchable Anonymous Attribute Based Encryption. In International Conference on Mathematics and Computing, Communications in Computer and Information Science book series (CCIS), vol. 655, Springer, pp. 16-25,2017

[18] J. Shi, J. Lai, Y. Li, R. H. Deng, and J. Weng. Authorized keyword search on encrypted data. In Proceedings of Computer Security, LNCS 8712, Springer, pp. 419-435, 2014.

[19] H. Wang, X. Dong, and Z. Cao. Multi-value-Independent Ciphertext-Policy Attribute Based Encryption with Fast Keyword Search. In IEEE Transactions on Services Computing, 99, 2017.

[20] P. Chaudhari and M. L. Das. A2BSE: Anonymous At- tribute Based Searchable Encryption. In Proceedings of ISEA Asia Security and Privacy Conference, IEEE, 2017.

[21] D. Cash, P. Grubbs, J. Perry, T. Ristenpart. Leakage- abuse attacks against searchable encryption. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, ACM, pp. 668–679, 2015.