International Journal for Modern Trends in Science and Technology, 8(05):53-57, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0805009
Available online at: http://www.ijmtst.com/vol8issue05.html

A Multi-Keyword Ranked Search Scheme for Encrypted Cloud Data

T Venkata Nikhil[1] | N Durga Devi[2] | L V Kiran[2]

[1]PG Scholar, Dept of CA, Godavari Institute of Engineering and Technology (A),Rajahmundry,A.P
[2]Assistant Professor, Dept of CA, Godavari Institute of Engineering and Technology (A),Rajahmundry,A.P
Corresponding Author Email ID: nikhiltavva4005@gmail.com[1], durgadevi.ansh@giet.ac.in[2], lvkiran@giet.ac.in[2]

To Cite this Article
T Venkata Nikhil, N Durga Devi and L V Kiran. A Multi-Keyword Ranked Search Scheme for Encrypted Cloud Data. International Journal for Modern Trends in Science and Technology 2022, 8(05), pp. 53-57. https://doi.org/10.46501/IJMTST0805009

Article Info
Received: 26 March 2022; Accepted: 25 April 2022; Published: 29 April 2022.

ABSTRACT

There are several advantages to cloud computing for both the individual and the community as a whole because of its flexibility and convenience. However, since shared data typically contains significant information, users have a natural reluctance to send it to the cloud server directly. Consequently, the shared data must be protected by an additional level of encryption. Identity-based encryption is a potential cryptographic basic that may be used to develop a viable data-sharing system. But access control is not a static issue. That is, if a user's authorization has expired, there should be a means to remove them from the system. To put it another way, the previously and later shared data is no longer accessible to a user who has had access revoked. As a result, this system offer RS-IBE, a concept that combines user revocation and ciphertext update functionality concurrently to guarantee ciphertext forward/backward security in real-time. Furthermore, this system describe an actual implementation of RS-IBE and establish its security under the stated security model. Because of its benefits in terms of both functionality and efficiency, the suggested RS-IBE data-sharing system is a viable option. In the end, we provide the outcomes of the execution of the suggested plan in order to illustrate its viability.

KEYWORDS: Cloud Computing, Ciphertext, Encryption, Cryptographic, RS-IBE.

1. INTRODUCTION

Cloud computing is a concept that provides vast processing power and massive memory space at a low cost. Users of the cloud benefit greatly from the ability to get the services they need at any time and from any location thanks to cloud computing[1,2]. Cloud storage systems like Apple's iCloud, Microsoft's Azure, and Amazon's s3 provide for more flexibility and simplicity of sharing data over the Internet. Many cloud users are hesitant about utilizing this service because of the security dangers[9]. Data is no longer within the control of the users while using a cloud server. Concerns may arise from the fact that outsourced data typically includes sensitive information. Cloud servers are an obvious target for attackers because of the open and adversarial nature of data sharing. Cloud servers may unlawfully profit from divulging users' sensitive info. Finally, the interchange of information is fluid. Data should be unavailable to a user after the user's authorization has expired. Many users now choose cloud storage since they can guarantee that only those who have been allowed access are able to see the data. Identity-based encryption[20], for example, is a reasonable answer to the difficulty outlined above (IBE). In order to protect shared

data from the threats outlined above, identity-based access control must also meet the following security objectives: No one except authorized users should be able to see shared data's raw text on a cloud server to ensure its privacy. Among other things, the cloud server, which is supposed to be honest yet inquisitive, should not know all of the shared content. Users should be unable to read the plaintext of encrypted material that they have shared with others after their authorization has expired or their secret key has been compromised[12]. Access to shared data in its plaintext should no longer be possible if an individual's authorization or secret key has expired or has been compromised for some other reason.

2. PROPOSED SYSTEM

In order to develop a cost-effective data sharing system that fulfils the three security requirements, it has been suggested to construct a system known as revocable storage identity-based encryption (RS-IBE), which is based on the concept of revocable storage identity-based encryption. The physical architecture of RS-IBE, as well as the formal definitions of RS-IBE and the security model that goes along with it, are all shown. It is proved that the suggested system may guarantee both confidentiality and backward/forward2 secrecy at the same time by making use of the decisional l-Bilinear Diffie-Hellman Exponent (l-BDHE) assumption. Moreover, it is proved that the suggested technique is safe in the standard model when the backward/forward2 secrecy assumption is used. Another feature of the suggested approach is that it is resistant to the disclosure of the decryption key, which is a significant advantage.

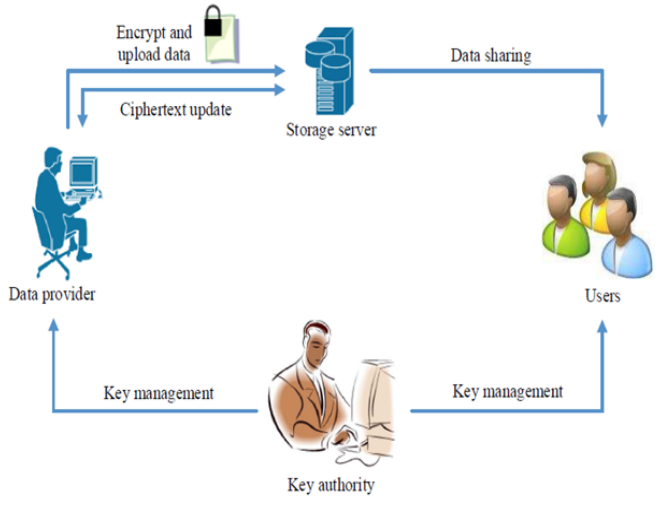


Figure 1: Proposed System Architecture

3. MODULE DESCRIPTION

CLOUD SERVER

Data owners, users, files, file requests, and all history may be seen on a cloud server. He has access to the personal information of every person who has registered with the system. Every user's information is available to him. He has access to all of the files that have been posted by the data owners. Whenever a user asks for a file, he sees it. Keys for file requests are sent to the user's email address by him. Also, he has access to all of the files that have been posted and downloaded in the past. For security reasons, he is the only person who can revoke the file's encryption keys.

DATA OWNER

First, the new Data Owner must complete the registration process by providing the requested information. After he logs in, he has the ability to upload and view files, as well as access to other users. He uses the internet to save his data on the cloud. He checks out the files he's just posted. All people who have signed up are visible to him.

USER

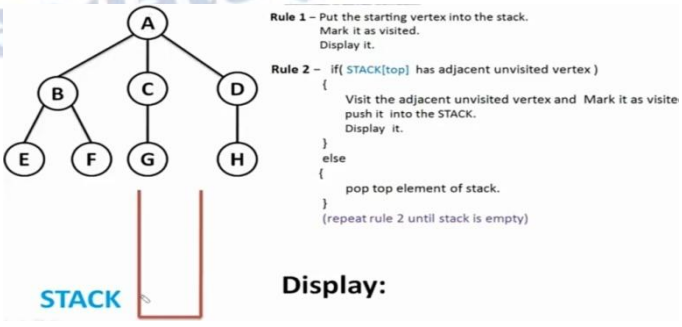
To begin, a new user must first provide the requested information in order to create an account on our site. After he logs in, he has the ability to view, transmit, and download files. His cloud storage files are visible to him. He makes a request for the file to the cloud server since he is interested in it. If the cloud server agrees to his request, a message containing file keys is delivered to the user's email address. Using the keys, he may access the file. If the cloud server revokes the file keys, the user will be unable to download the files. He has to ask for the key once again.

4. ALGORITHM

Depth-first search is an algorithm for traversing or searching tree or graph data structures.

It Uses stack data structure (LIFO-Last In First Out).

It traverses a graph or tree in a depth ward motion.



5. EXPERIMENTAL RESULTS

Users, files, and file requests are tracked by a cloud server. He has access to every user's data. All users' info is available. He has access to all data owners' files. He views a file when a user asks. The user submits file key requests through email. Accessed previous files supplied and downloaded. The file's encryption keys are only his. Begin by filling out a registration form with the required details. After signing on, he may see other users' files and upload them. He uses the internet to store data. He downloads his files. He can see who signed up. A new user must first register. He can then view files, request files, and download files. He sees cloud files. He asks the cloud server for the file he wants. The cloud server responds by sending an email to the user's address. He can get the key file. In this case, the user can't download. He must re-apply.

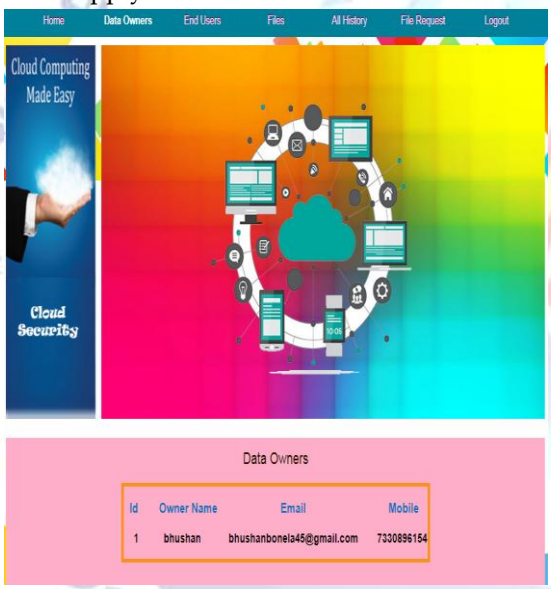


Fig5.1: View Data Owners

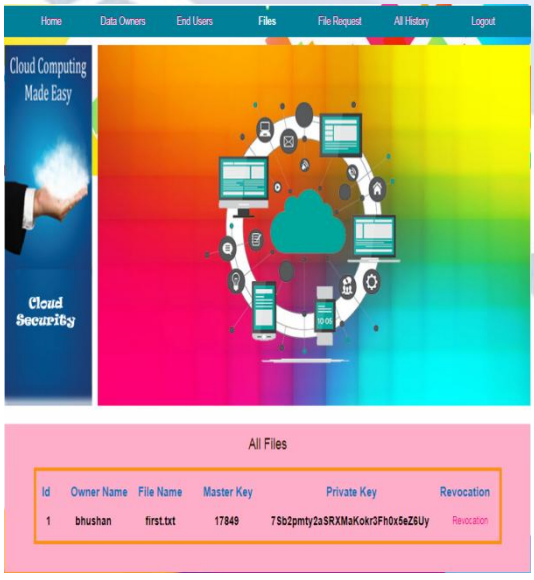


Fig5.2: View All Files

Fig5.3: View All Process

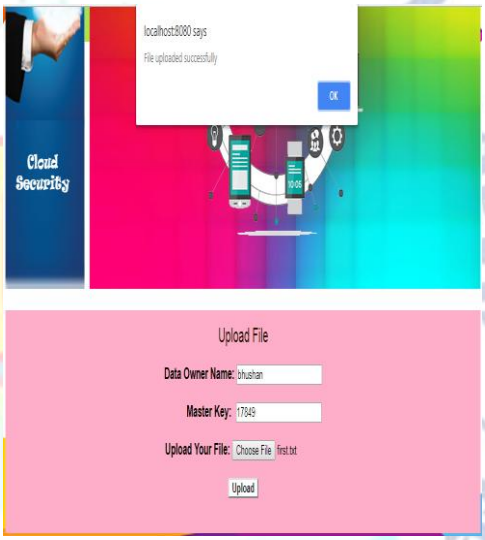


Fig5.4: Upload File

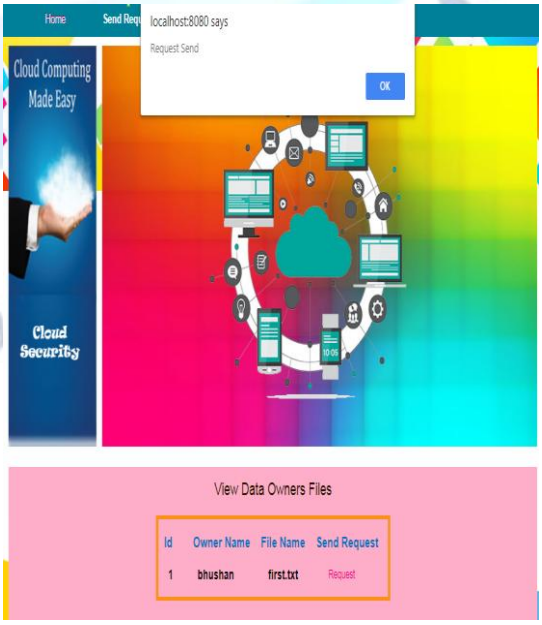


Fig5.5: View Data Owner Files

Fig5.6: View End Users

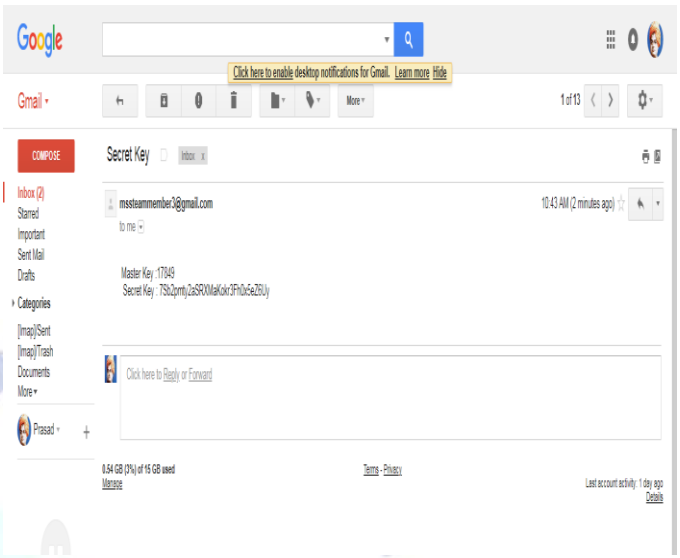


Fig5.7: Secret Key

6. COMPARATIVE STUDY

Table 1 lists three keyword classes with varying IDF values. The lower the IDF number, the more common the keyword. Table 1 illustrates that adding or removing 100 or 300 documents has no effect on IDF results. The data owner does not need to adjust IDF values every time he updates the dataset. When IDF values vary a lot, the data owner might choose to check for changes and disseminate the new values.

Table 1: Comparative Study

Keyword NO	Original IDF values	IDF values in the updated collection			
		After deleting 100 documents	After deleting 300 documents	After adding 100 documents	After adding 300 documents
1	3.0332	3.0253	3.0166	3.0334	3.0267
2	3.2581	3.2581	3.2530	3.2628	3.2857
3	3.7616	3.7584	3.7431	3.7647	3.7550
4	3.8934	3.8926	3.8910	3.9128	3.9226
5	5.6304	5.6103	5.6861	5.6501	5.6885
6	5.7478	5.7277	5.6861	5.7675	5.8059
7	5.8121	5.7920	5.8192	5.8319	5.8702
8	7.4192	7.3990	7.3573	7.4390	7.4774
9	7.8244	7.8043	7.7626	7.8442	7.8827
10	8.5174	8.4972	8.4555	8.5372	8.5757

7. CONCLUSION

Many people's lives have been made easier by the advent of the cloud. As a result, it is well suited to the increasing need for data exchange through the Internet. In order to create a cloud computing data sharing system that is both cost-effective and secure, this system proposed a concept called RS-IBE, which supports both identity revocation and ciphertext update at the same time, preventing a revoked user from accessing previously shared data as well as data that has been shared since. It's also shown how to build the RS-IBE system in real time. Assuming the decisional l-DBHE assumption, an adaptive-secure RS-IBE technique may be developed. Results from a comparative study show that our method is more efficient and useful, making it a better choice for real-world applications.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

[2] iCloud. (2014) Apple storage service. [Online]. Available: https://www.icloud.com/

[3] Azure. (2014) Azure storage service. [Online]. Available: http://www.windowsazure.com/

[4] Amazon. (2014) Amazon simple storage service (amazon s3). [Online]. Available: http://aws.amazon.com/s3/

[5] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," Services Computing, IEEE Transactions on, vol. 5, no. 4, pp. 551–563, 2012.

[6] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

[7] G. Anthes, "Security in the cloud," Communications of the ACM, vol. 53, no. 11, pp. 16–18, 2010.

[8] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.

[9] B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in INFOCOM, 2013 Proceedings IEEE. IEEE, 2013, pp. 2904–2912.

[10] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384–394, 2014.

[11] X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "Cost-effective authentic and anonymous data sharing with forward security," Computers, IEEE Transactions on, 2014, doi: 10.1109/TC.2014.2315619.

[12] C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 468–477, 2014.

[13] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in cryptology. Springer, 1985, pp. 47–53.

[14] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, 2003.

[15] S. Micali, "Efficient certificate revocation," Tech. Rep., 1996.

[16] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology–CRYPTO 1998. Springer, 1998, pp. 137–152.

[17] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in Advances in Cryptology–CRYPTO 2001. Springer, 2001, pp. 41–62.

[18] C. Gentry, "Certificate-based encryption and the certificate revocation problem," in Advances in Cryptology–EUROCRYPT 2003. Springer, 2003, pp. 272–293.

[19] V. Goyal, "Certificate revocation using fine grained certificate space partitioning," in Financial Cryptography and Data Security. Springer, 2007, pp. 247–259.

[20] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proceedings of the 15th ACM conference on Computer and communications security. ACM, 2008, pp. 417–426.

[21] M. Naor and K. Nissim. Certificate Revocation and Certificate Update. In USENIX Security Symposium, 1998.

[22] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure attribute-based systems. In ACM Conference on Computer and Communications Security, pages 99–112, 2006.

[23] A. Sahai and B. Waters. Fuzzy Identity-Based Encryption. In EUROCRYPT, pages 457–473, 2005.

[24] A. Shamir. Identity-Based Cryptosystems and Signature Schemes. In CRYPTO, pages 47–53, 1984.

[25] B. Waters. Efficient Identity-Based Encryption Without Random Oracles. In EUROCRYPT, pages 114–127, 2005.

[26] P. Yang, T. Kitagawa, G. Hanaoka, R. Zhang, K. Matsuura, and H. Imai. Applying FujisakiOkamoto to Identity-Based Encryption. In AAECC, pages 183–192, 2006.