ISSN: 2278-4632
Vol-10 Issue-5 No. 14 May 2020

An Efficiency of Encryption Data to Provide Security by Using Cloud Computing

Dr .P. Kalyani,

Professor, Department of MCA, Narayana Engineering College-Gudur Nellore dist, AP.

J. Akash,

PG scholar Department of MCA from Narayana Engineering college- Gudur, Nellore dist, AP.

Abstract: If the Cipher text strategy point is based encryption can provide fine granuled contact control and secure data sharing to the data clients in CC (Cloud Computing). If the How ever if the encryption or decryption is efficiency of the existing schemes is can be extra developed. Then the encrypting is a large documentation collection.Where In this project we can propose the practical Cipher text of the Policy Attribute is based on Hierarchical document and collection of Encryption scheme named is also CP-ABHE. If the practical is we can mean that the CP-ABHE is also more efficient and the both computation and also storage of the space without of the sacrificing of the data security. In this greatly the improves of the performance is also the CP-ABHE. The Simulation results isalso illustrate of that are to CP-ABHE performs of very well then the in terms of the security are efficiency and also the storage size is the cipher text.

Key words: information security, cloud computing, Information technology, Attribute based file collection encryption, encryption/decryption efficiency

I. Introduction

The cloud computing collects and organizes a huge quantity of notification technique resources to provide secure, efficient, flexible and on demand services. At tracted by these advantages, more and more enterprise and individual users trend to outsource the local documents to the cloud. In general, the documents need to be encrypted before being outsourced to protect them against leaking. Then the data owner is to wantsto share thesetypes of documents with an authorized of data user.

Then they can employ ofany searchable to encryption techniques or privacy preserving of multi keyword document is search schemes to achieve of this goal. Whenever, of all these schemes is also cannot provide the finegrained of access the control mechanisms of the encrypted documents. Attribute based encryption schemes can be providing complicated of systems to the diver of the data users access paths. In ABE schemes, of every file is encrypted of individuallyand the data user can be decrypt of a document if their attribute is set to matches the access of construction of the file.

II. Related works

Attracted by these advantages, more and more enterprise and individual users trend to outsource the local documents to the cloud.In general, the documents need to be encrypted before being outsourced to protect them against leaking.Whenever all these schemes we cannot provide the fine grained accessthe control mechanisms is to the encrypted of documents.Then the design of the inputis focuses on the controlling of

ISSN: 2278-4632
Vol-10 Issue-5 No. 14 May 2020

the amount of input required.The controlling of the errors and avoiding delay, avoiding the extra steps and the keeping of the process simple.So thistype design is important of avoid errors in the data of input process and show that the correct direction of the management of getting correct information from that the computerized system.

III. Proposed work

A document collection hierarchical encryption scheme is proposed. Which can significantly improve the encryption or decryption efficiency.Moreover, the secret key expanding problem is solved properly.The security of CP-ABHE is theoretically proved and the effectiveness of the integrated access tree construction algorithm is analyzed in detail. In addition, a thorough comparison between CP-ABHE, KP-ABE, and CP-ABE in terms of encryption or decryption efficiency and storage space is provided. If theSimulation of results is to be illustrate of that the CP ABHE is also performs is extremely good in phrases of the security and efficiency. In this project then the data is stored in the cloud computing is very fast by using that the CP-ABHE.

IV. Analysis

By using in this section, we are mainly focus on our attention and analyzing of the security of the CP ABHE and the other security problems in that document retrieval of system are the out of scope in this project. Specifically, then the documents are encrypted based on the symmetric encryption schemes and they are assumed to the secure if the content keys are secure. Then, we mainly restrict our attention to the security of the content keys in CP ABHE. we prove the security the of CP ABHE under the Selective Set Security Game is based on the Decisional BDH assumption to provided in this Section.

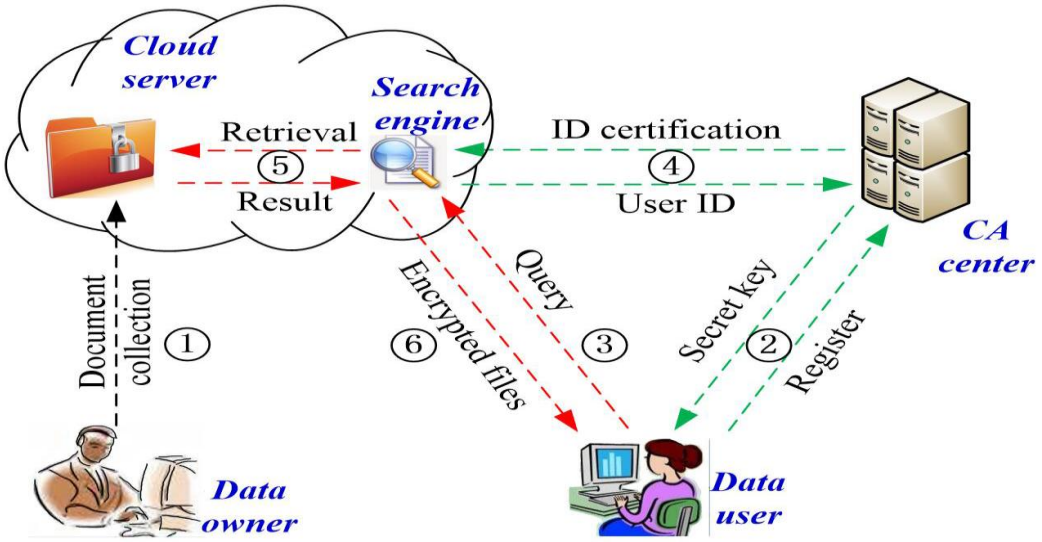

FIGURE 1. The architecture of document outsourcing and sharing

V. Experiment Results

ISSN: 2278-4632
Vol-10 Issue-5 No. 14 May 2020

Attribute-based encryption schemes have been widely re- searched in the literatures. The fuzzy identity-based encryption (Fuzzy IBE) scheme proposed by et al is widely treated as the origin of attribute-based encryption (ABE). al first employ the term “attribute-based encryption (ABE)” in the field of information security. Inspired by Fuzzy IBE, many ABE schemes are designed including KP-ABE schemes and CP-ABE schemes. Goya extend the Fuzzy IBE scheme and propose the key-policy attribute- based-encryption (KP-ABE) . Though KP-ABE can provide fine-grained access control, it restricts its attention to the monotone access structure only. In, construct a KP-ABE scheme which allows a user’sprivate key can be expressed in terms of any access formula over attributes. Further, they prove the scheme’s security based on decisional bilinear Hellman assumption.

|A|

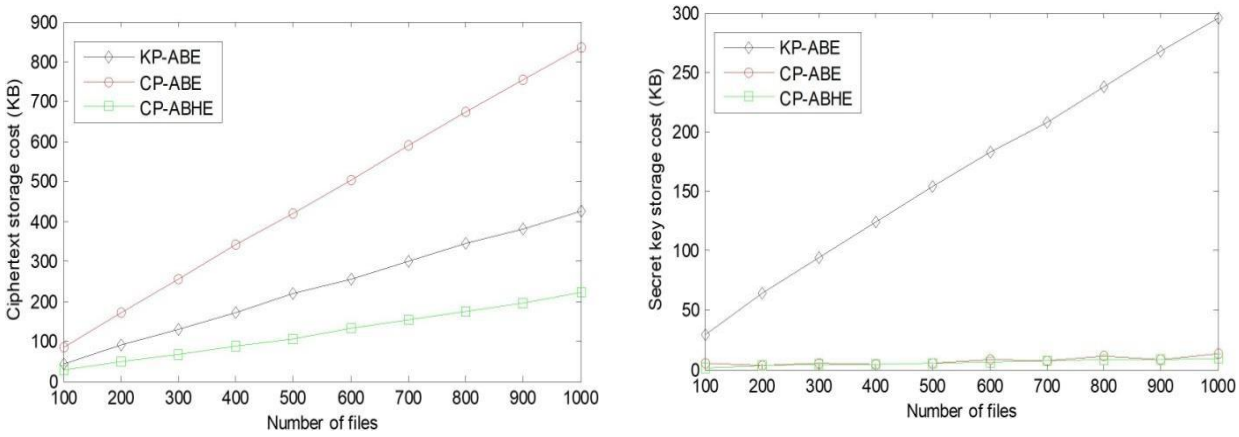

FIGURE 2. Ciphertext storage space.

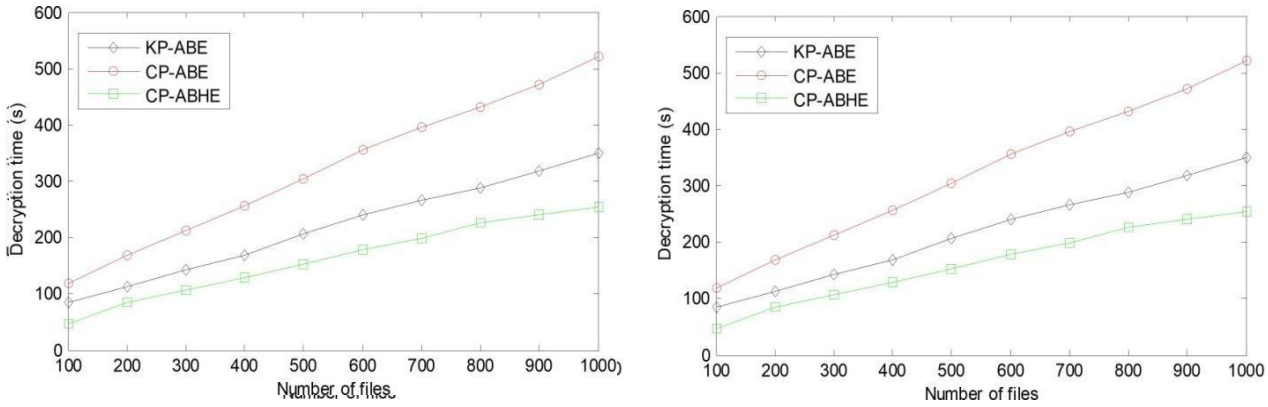

FIGURE .3: Decryption time.

VI. Conclusion

ISSN: 2278-4632
Vol-10 Issue-5 No. 14 May 2020

In this paper, we design a hierarchical document collection encryption scheme. We first design an incremental algorithm to construct the integrated access trees of the documents and decrease the number of trees. Then, each integrated access tree is encrypted together and the documents in a tree can be decrypted at a time. Different to existing schemes, we construct the secret numbers for the nodes of the trees in a bottom-up manner. In this way, the sizes of ciphertext and secret keys significantly decrease. At last, a thorough performance evaluation is provided including security analysis, efficiency analysis, and simulation. Results show that the proposed scheme outperforms KP-ABE and CP-ABE schemes in terms of encryption/decryption efficiency and storage space.

References:

1. J. Han, W. Susilo, Y. Mu, et al., "Privacy-Preserving Decentralized Key- Policy Attribute-Based Encryption," IEEE Transactions on Parallel & Distributed Systems, 2012.
2. D. Boneh, B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc. of TCC, 2007, pp. 535-554.
3. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi- keyword ranked search over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222-233, Jan. 2014.
4. A. D. Caro, V. Iovino, "jPBC: Java pairing based cryptography," IEEE Symposium on Computers and Communications. IEEE Computer Society, 2011:850- 855.
5. C. Chen et al., "An efficient privacy-preserving ranked key-word search method," IEEE Trans. Parallel Distrib. Syst., vol. 27, no, 4, pp. 951-963, Apr. 2016.
6. P Penchalaiah, M Vijay Kumar etl, "A Research Threshold Efficient Hybrid Encryption Schema for Secure File System", International Journal of Recent Technology and Engineering (IJRTE),ISSN: 2277-3878, (SCOPUS) Volume-8, Issue-2S3, Page 888 – 891,July 2019
7. R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. ACM CCS, 2006, pp. 79-88.
8. Rajasekar, P. and Mangalam, D. (2016) Efficient FPGA implementation of AES 128 bit for IEEE 802.16e mobile WiMax standards. Circuits and Systems, 7, 371-380. doi: 10.4236/cs.2016.74032.
9. H. Deng, Q. Wu, B. Qin, et al., "Ciphertext-policy hierarchical attribute- based encryption with short ciphertexts," Information Sciences, 2014, 275(11):370- 384.
10. Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 9, pp. 2546-2559, Sep. 2016.
11. P. Golle, J. Staddon, B. Waters, "Secure conjunctive key-word search over encrypted data," in Proc. of ACNS, 2004, pp. 31-45.
12. V. Goyal, A. Jain, O. Pandey, et al., "Bounded ciphertext policy attribute based encryption," Automata, languages and programming, 2008: 579- 591.

Author's profile:

Dr.P.Kalyani, Proffessor, Department of MCA,Narayana Engineering College Gudur. She received her MCA from Sri Venkateswara University-Tirupati in 2006.Ph.D from Sri Venkateswara University –Tirupati in 2018.Her areas of Research: Spatial Data mining,Remote sensing,GIS,IOT.

J.Akash has received his degree from Sri Vema degree college, Nayudupeta which is affiliated to Vikrama Simhapuri University Nellore in 2015-2018. Now Persuing MCA at Narayana Engineering college-Gudur which is affiliated to JNTU Anantapuram.

