Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

An Effective CP-ABE Scheme Using Shared Decryption for Cloud Storage

R.RAMAIAH [1], K. SUDHAKAR [2]

[1] PG Scholar, Dept of CSE, Gokula Krishna College of Engineering, Sullurpeta, AP, India.

[2] Assistant Professor, Dept of CSE, Gokula Krishna College of Engineering, Sullurpeta, AP, India.

ABSTRACT_ Attribute-based encryption (ABE) is a favoured way for managing access to cloud server data. The authorised decryption user, on the other hand, may not always be able to decrypt the ciphertext in a timely manner. To ensure security, numerous alternate users are allocated to decrypt the ciphertext rather than just one. We introduce a shared decryption ciphertext-policy ABE technique in this paper. An authorised user can recover the mails on their own. These additional clients (semi-approved clients) can work together to receive messages at the same time. We also work on the essential strategy to ensure that the semi-approved consumers carry out the unscrambling errands legitimately. The use of an integrated access tree improves the efficiency of our strategy. The standard model shows that the new technique is CPA-safe. The experimental results suggest that our strategy is quite productive in terms of both computational above and capacity cost..

1.INTRODUCTION

Distributed storage [1,2] is another capacity innovation in light of organization and distributed computing, which gives "limitless" capacity assets for information clients. The cloud-based data can be easily accessed by users from any location. Cloud storage servers are storing more personal and business data. By storing their data on the remote cloud storage servers, these businesses and individuals can significantly reduce the cost of data storage and management. In any case, the cloud specialist co-op, for example, Google Cloud, IBM Cloud, and Microsoft Cloud, might be interested or benefit headed to release clients' delicate information. Furthermore, these information put away on remote distributed storage servers might be gone after, altered, and unveiled by programmers. As a result, before storing their files on an unreliable cloud storage server, users typically encrypt them. To guarantee the accuracy of the documents, a

few far off information trustworthiness checking plans [3-7] were proposed. However, there are still issues with the data for cloud storage [8].

In recent years, attribute-based encryption (ABE), which has the potential to guarantee data stored on cloud servers' privacy, has become a hot cryptography research topic. Sahai and co. 9] proposed the idea of ABE as an extension of the previous identity-based encryption. An attribute set replaces a user's identity in the presented ABE. There are two types of current ABE schemes: ciphertext-policy ABE (CP-ABE) and key-policy ABE (KP-ABE) schemes. Goyal et al. [10] implemented a KP-ABE plan in 2006. In this plan, an entrance structure is connected with the confidential key of a client. A ciphertext-related attribute set exists simultaneously. In 2007, Bethencourt et al. [11] offered a CP-ABE plan. His plan is more reasonable and more adaptable than KP-ABE conspire. In a CP-ABE conspire, a quality set is connected with the confidential key of the client, while an entrance structure is connected with the code text. The cipher text can only be decrypted by a user whose attribute set meets the access policy.

2. LITERATURE SURVEY

2.1) S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, "Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 337–368, 2014.

Recently, Cloud-based Mobile Augmentation (CMA) approaches have gained remarkable ground from academia and industry. CMA is the state-of-the-art mobile augmentation model that employs resource-rich clouds to increase, enhance, and optimize computing capabilities of mobile devices aiming at execution of resource-intensive mobile applications. Augmented mobile devices envision to perform extensive computations and to store big data beyond their intrinsic capabilities with least footprint and vulnerability. Researchers utilize varied cloud-based computing resources (e.g., distant clouds and nearby mobile nodes) to meet various computing requirements of mobile users. However, employing cloud-based computing resources is not a straightforward panacea. Comprehending critical factors (e.g., current state of mobile client and remote resources) that impact on augmentation process and optimum selection of cloud-based resource types are some challenges that hinder CMA

adaptability. This paper comprehensively surveys the mobile augmentation domain and presents taxonomy of CMA approaches. The objectives of this study is to highlight the effects of remote resources on the quality and reliability of augmentation processes and discuss the challenges and opportunities of employing varied cloud-based resources in augmenting mobile devices. We present augmentation definition, motivation, and taxonomy of augmentation types, including traditional and cloud-based. We critically analyze the state-of-the-art CMA approaches and classify them into four groups of distant fixed, proximate fixed, proximate mobile, and hybrid to present a taxonomy. Vital decision making and performance limitation factors that influence on the adoption of CMA approaches are introduced and an exemplary decision making flowchart for future CMA approaches are presented. Impacts of CMA approaches on mobile computing is discussed and open challenges are presented as the future research directions

2. 2) Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption

AUTHORS: Jung, T., Li, X. Y., Wan, Z. and Wan, M

Although some cloud servers store data, which raises a number of privacy concerns, cloud computing is a revolutionary computing paradigm that enables flexible, on-demand, and low-cost resource utilization. To protect cloud storage, a number of approaches based on attribute-based encryption have been proposed. However, identity privacy and privilege control receive less attention than data content privacy and access control in most projects. AnonyControl, a semi-anonymous privilege control method, is presented in this paper to address the data privacy and user identity privacy concerns of existing access control methods. To prevent identity leaks, AnonyControl decentralizes authority, resulting in semi-anonymity. In addition, it extends file access control to privilege control, making it possible to fine-tune privilege management for all cloud data operations. Then, we present the AnonyControlF, which achieves complete anonymity and completely prevents identity leakage. Our performance evaluation demonstrates the viability of our schemes, and our security analysis demonstrates that, under the DBDH assumption, both AnonyControl and AnonyControl-F are secure.

3.PROPOSED SYSTEM

The proposed system presented the CP-ABE with shared decryption (CP-ABE-SD) approach to address the aforementioned issue. In our solution, many delegated users may collaborate with the authorised user to recover the message. We can confirm the accuracy of the decryption results at the same time. In our approach, as in the scheme, an integrated access tree is employed to reduce the computation cost for encryption and decryption and to save storage expenses. Finally, the plaintext is encrypted via the integrated access tree. Because it necessitates frequent data encryption and decryption procedures, cloud storage is inefficient. The shared communication is encrypted only once by our system, and the ciphertext is little. Our approach improves the efficiency of cloud storage.

3.1 IMPLEMENTATION

- **Data Owner**

In this module, the data provider uploads their encrypted data in the Cloud server. For the security purpose the data owner encrypts the data file and then store in the server. The Data owner can have capable of manipulating the encrypted data file and performs the following operations Register and Login, Add Document, View Uploaded and Verify Details.

- **Cloud Server**

The **Cloud** server manages which is to provide data storage service for the Data Owners. Data owners encrypt their data files and store them in the Server for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the Server and then Server will decrypt them. The server will generate the aggregate key if the end user requests for file authorization to access and performs the following operations such as Login, Attackers, Authorize User, Authorize Owner, View Documents, Top Searched Keywords, Search Keyword Chart,
View File Rank Chart .

User

In this module, the user can only access the data file with the secret key. The user can search the file for a specified keyword. The data which matches for a particular keyword will be indexed in the cloud server and then response to the end user and user will do the following operations Register and Login, Search, My Profile, View Files, Request Secret Key and Public Key Permission, Request Hash Key Permission.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

- **Trusted Authority** –is responsible for Login, View Files, View Transactions, Generate Hash Code, View Keys Requests and Permit**.**

.

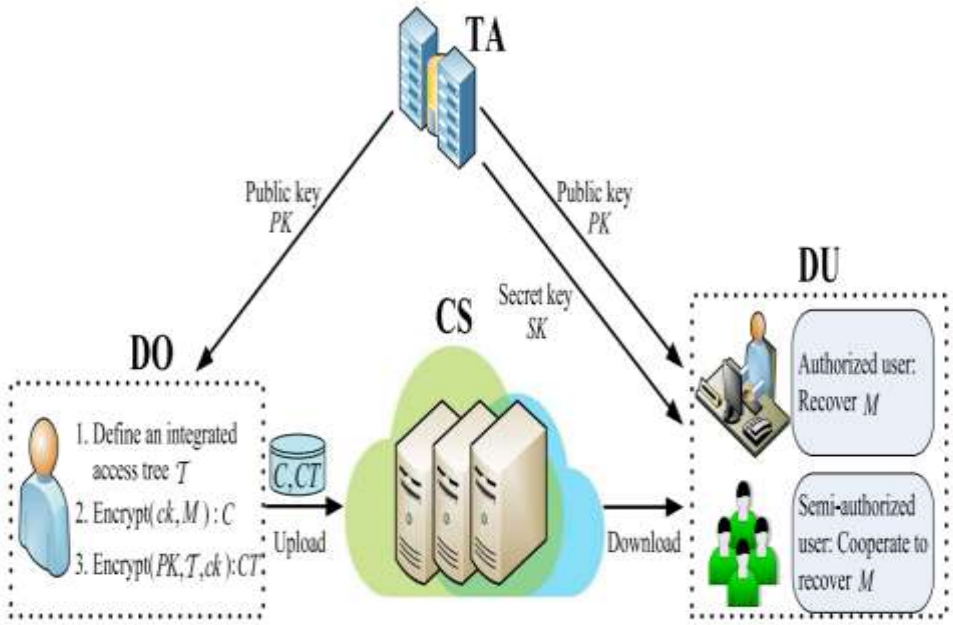
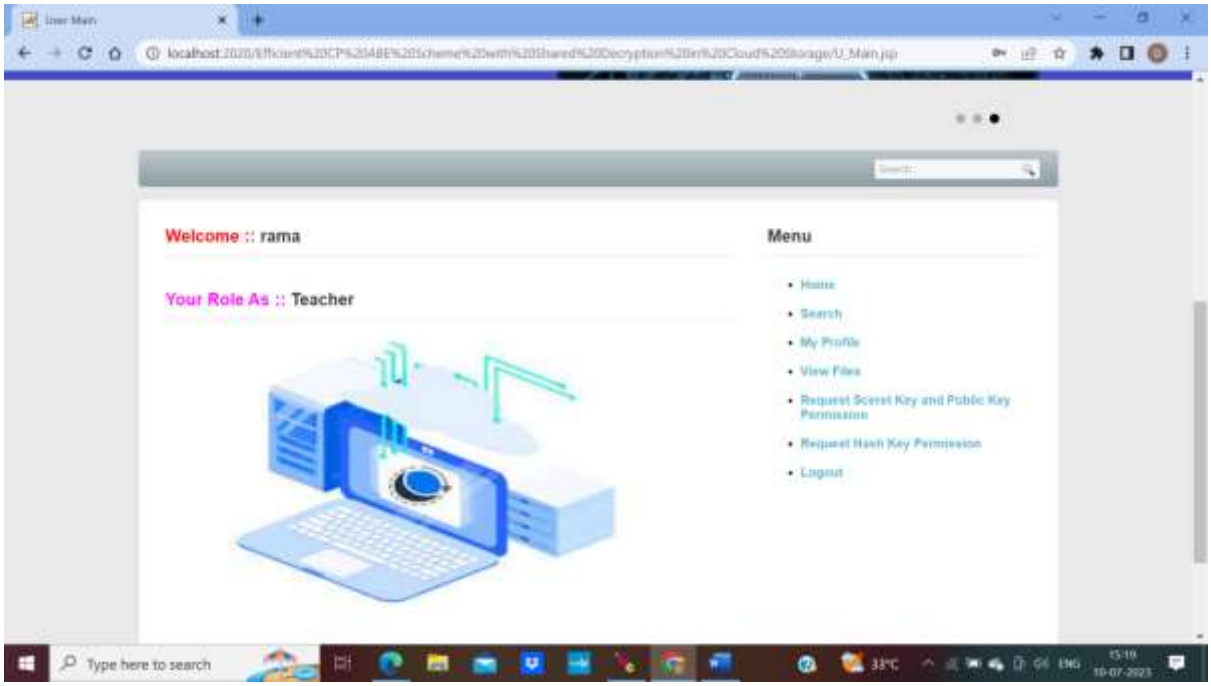


Fig 1: Architecture

4. RESULTS AND DISCUSSION



Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

Fig 2:User Home Page

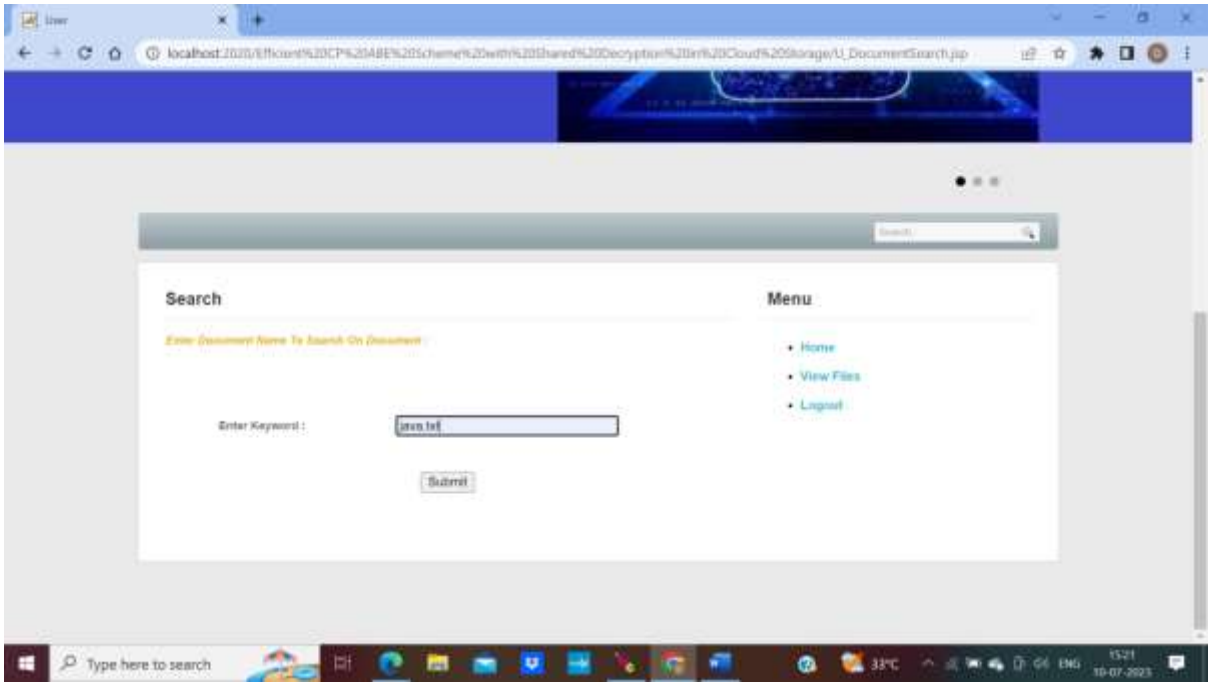


Fig 3:User Search For data

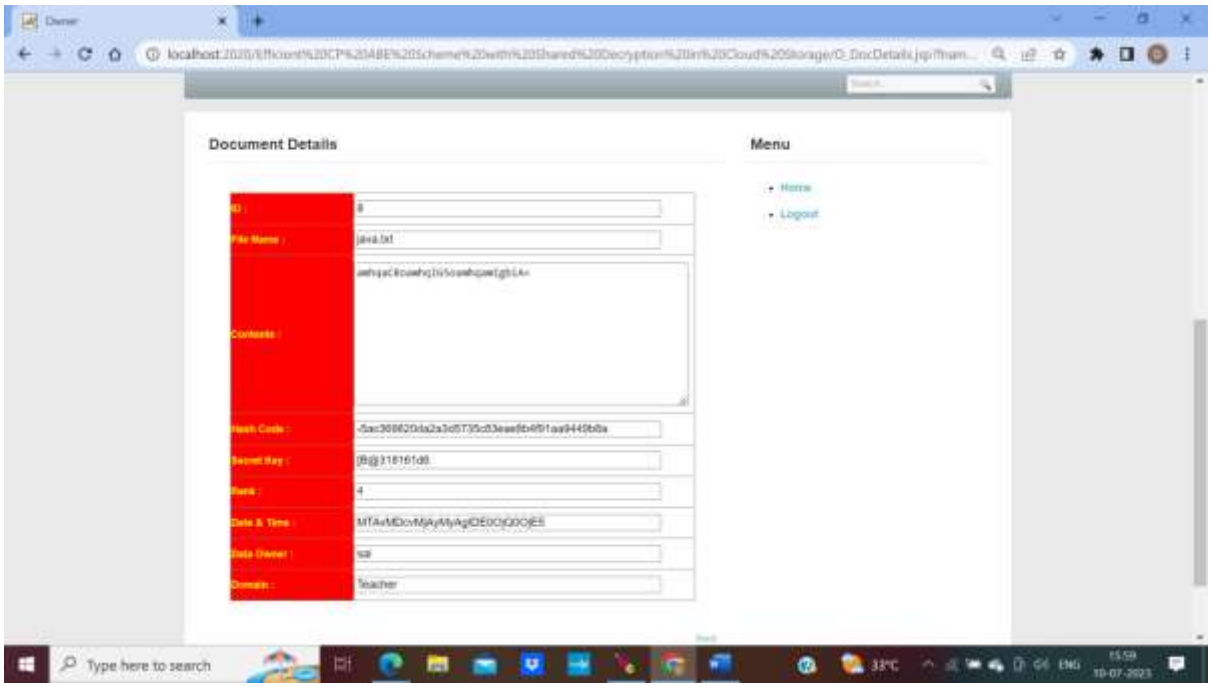


Fig 4:Data owner uploaded data in the form of ncryption

5. CONCLUSION

We provide two encryption techniques that share decryption and leverage cypher text-policy features. There are two categories of data users in our systems. The message can be recovered by an approved user on their own. These semi-authorized users can collaborate to decrypt the cypher text in place of the authorised user if the authorised user is unable to do so in time for whatever reason. An integrated access tree is used to improve the efficiency of the suggested schemes. Our schemes' security has been demonstrated under the DBDH assumption. The experimental results show that the CP-ABE-SD scheme beats the other methods in terms of storage cost and computational overhead.

REFERENCES

[1] S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, “Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 337–368, 2014.

[2] J. Aikat et al., “Rethinking security in the era of cloud computing,” *IEEE Security Privacy*, vol. 15, no. 3, pp. 60-69, Jun. 2017.

[3] J. Li, H. Yan, and Y. Zhang, "Efficient identity-based provable multi-copy data possession in multi-cloud storage," *IEEE Transactions on Cloud Computing*, DOI: 10.1109/TCC.2019.2929045.

[4] J. Li, H. Yan, and Y. Zhang, “Certificateless public integrity checking of group shared data on cloud storage,” *IEEE Transactions on Services Computing*, to be published. DOI 10.1109/TSC.2018.2789893.

[5] H. Yan, J. Li, and J. Han, “A novel efficient remote data possession checking protocol in cloud storage,” *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 78-88, Jan. 2017.

[6] H. Yan, J. Li, and Y Zhang, “Remote data checking with designated verifier in cloud storage,” *IEEE Systems Journal*, vol. 14, no. 2, pp. 1788-1797, 2020.

[7] J. Li, H. Yan, and Y. Zhang, “Identity-based privacy preserving remote data integrity checking for cloud storage,” *IEEE Systems Journal*. DOI:10.1109/JSYST.2020.2978146.

[8] L. Zhang, H. Xiong, Q. Huang, J. Li, K. K. Raymond Choo, and J. Li, "Cryptographic solutions for cloud storage: challenges and research opportunities," *IEEE Transactions on Services Computing*, DOI: 10.1109/ TSC.2019.2937764.

[9] A. Sahai and B. Waters, "Fuzzy identity based encryption," *Advances in Cryptology-Eurocrypt 2005, Lecture Notes in Computer Science, vol. 3494, Springer, 2005*, pp. 457-473.

[10] V. Goyal, O. Pandey, A. Sahai, and Brent Waters, "Attribute-based encryption for fine-grained access control of encrypted data," *Proc. 13th ACM Conference on Computer and Communications Security*, 2006, pp. 89–98.

[11] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," *IEEE Symposium on Security and Privacy*, vol. 2008, pp. 321-334, Jun. 2007.

[12] J. Lai, R. H. Deng, and Y. Li, "Expressive CP-ABE with partially hidden access structures," *Proc. 7th ACM Symposium on Information, Computer and Communications Security*, pp. 18-19, 2012.

[13] S. Yu, K. Ren, and W. Lou, "Attribute-based content distribution with hidden policy," *Proc. IEEE 4th Workshop on Secure Network Protocols*, pp. 39-44, 2008.[14] N. Doshi and D. Jinwala, "Hidden access structure ciphertext policy attribute based encryption with constant length ciphertext," *IEEE international Conference on Computer and Communication Technology*, Nov. 2011, pp. 515–523.

[15] J. Li, Y. Zhang, J. Ning, X. Huang, G. S.Poh, and D. Wang, "Attribute based encryption with privacy protection and accountability for cloudIoT," *IEEE Transactions on Cloud Computing*, 2019, DOI:10.1109/ TCC.2020.2975184.

[16] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," *Proc. 14th ACM conference on Computer and Communications Security*, pp. 121-130, 2009.

[17] H. Qian, J. Li, Y. Zhang, and J. Han, "Privacy preserving personal health record using multi-authority attribute-based encryption with revocation," *International Journal of Information Security*, vol. 14, no. 6, pp. 487–497, Nov. 2015.

[18] J. Li, W. Yao, J. Han, et al, "User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage," *IEEE Systems Journal*, vol. 12, no. 2, pp. 1767-1777, Jun. 2018.