IJMTST is UGC Approved Journal with Journal Id: 43137

International Journal for Modern Trends in Science and Technology, 8(S03):09-12, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST08S0303
Available online at: https://www.ijmtst.com/vol8si03.html

Secure and Efficient Attribute-Based Access Control for Multiauthority Cloud Storage

Dr. J.M.S.V. Ravi Kumar| M. Bhagya Sri | S. Tarun Kumar | A.S.V. Raghunandan | V. Gowtham

Department of Computer Ccience and Engineering, Godavari Institute of Engineering and Technology(A), JNTUK, Kakinada.

To Cite this Article
Dr.B Sujatha, K.Sri Lasya, N.NagaSuneetha Devi, A.Gnana Surya Bhavani Prasad and P.Dileep Surya Manikanta. Extraction of Text from Images using Machine Learning.International Journal for Modern Trends in Science and Technology 2022, 8(S03), pp. 09-12.https://doi.org/10.46501/IJMTST08S0303

Article Info
Received: 26 April 2022; Accepted: 24 May 2022; Published: 30 May 2022.

ABSTRACT

People and businesses alike benefit from cloud storage since it makes it easier to correctly share their data over the internet. As a result, there is a lot of room for error when it comes to managing the input of shared information. Here, we provide financial and ownership-based insights to regulate distributed storage infrastructures. There is no central authority and all real estate specialists independently issue mystery keys to clients; 2) each characteristic authority can gradually evict any customer from its space with the ultimate goal of such waived consumers not being able to obtain information redistributed in this manner; 3) cloud servers can update encoded information; and 3) we construct an inter-authority CPABE conspiracy

1.INTRODUCTION

Cloud computing developments have made it possible to store data from several clients on the cloud. Customers can save their data in the cloud from the comfort of their own homes or workplaces thanks to cloud computing. Increasing a company's memory is less expensive when a remote backup system is used[10]. Contribute to the reduction of data management costs in government and business. In place of owning and operating a data centre, companies can back up their data to third-party cloud storage services. Storage devices need not be purchased by an individual or a company. In the event of system failures, such as hardware or software breakdowns, they can save and preserve their data on the cloud to avoid data loss. Because of worries over security and privacy, storing outsourced data in the cloud is a big source of anxiety.

The cloud uses encryption to protect data flows. A cloud storage service must be used to keep encrypted files after they have been decrypted[11]. Even if they don't have the decryption key, it's possible for someone else to see the record. Cloud computing, a vast open distributed system, is one of the more recent technologies being explored to address this issue. Keeping users' personal information and internet privacy secure is essential.

As a result of attribute-based encryption, data owners have complete control over their data and granular control over who has access to their files in the public cloud. There are two types of ABE schemes that have been proposed so far: Key Policy Attribute Based Encryption (KPABE) and Cryptographic Text Policy Attribute Based Encryption (CTPABE) (CPABE). Using KPABE methods, decryption keys are linked to access structures, and the ciphertext is tagged with specific attribute sets so that attribute management and key distribution authority may be handled. The authority can be the human resources department of a firm, the register of a university, or another body. Access policies are specified by the data owner, who then encrypts their data

in compliance with those policies. For each user, they'll be given their own unique key, depending on their distinctive traits. In order for data to be decrypted, it must meet the policies for access.

A policy or approach that allows, denies or restricts access to a computer system is called "access control." Any attempts to access a computer are also logged by the system. Access control methods can be used to identify an unauthorised user who is attempting to get access to an IT system. This is a crucial step towards cybersecurity. Cloud storage is a critical component of cloud computing. Owners of data can store it in the cloud with the help of Cloud Storage. There are major challenges for data access control systems when it comes to the hosting and access of digital data. Data owners no longer have faith in cloud servers to enforce access controls on their behalf, making it impossible to maintain control over cloud storage systems. As a result, decentralised access control is implemented.

2. LITERATURE SURVEY

1) DAC-MACS: Effective data access control for multi-authority cloud storage systems

Data access control in the cloud is an effective method of securing data. Because of data outsourcing and unreliable cloud servers, securing access to cloud storage data is a difficult task. Traditional access control methods no longer work since cloud storage solutions do not make multiple encrypted copies of the same data or request a completely trusted cloud server. Restricting access to encrypted data is possible with the Ciphertext Policy Attribute-based Encryption (CPABE) technique. All system keys and attributes must be under the control of a trusted source. Each cloud storage authority has the ability to provide attributes on an individual basis. Traditional CPABE methods cannot be utilised to regulate access to multi-authority cloud storage systems due to inefficient decryption and revocation. An efficient and safe data access control method is provided here in the form of DACMACS (Data Access Control for Multi-Administrative Cloud Storage). An efficient decryption and an efficient attribute revocation method are included in the new multi-authority CPABE system we design. According to our observations and the results of our simulations and analyses, our DACMACS is highly effective and probably secure.

3. EXISTING SYSTEM

Attribute-based encryption (ABE) is considered one of the best methods for enforcing data access control in the public sector. the cloud because it provides data owners with direct control over their data and sophisticated access control. Two main categories of ABE schemes have been presented so far: Key Policy Attribute Based Encryption (KPABE) and Ciphertext Policy Attribute Based Encryption (CPABE).

KPABE methods link decryption keys to access structures, but ciphertexts are only given particular attribute sets as a means of identifying them. However, with CPABE schemes, data owners have the option of defining an access policy for each file depending on the user's attributes, which gives them more control over their information. For public cloud storage, CPABE is a better option than KPABE in terms of access control design..

4. PROPOSED SYSTEM

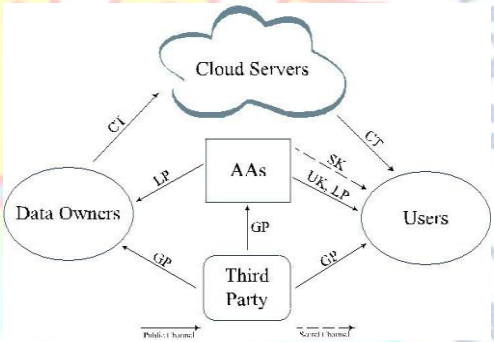

Fig 1: Architecture

1. Data Access Control Scheme:

For the sake of security and performance, we present a multi-authority CPABE access control mechanism that is resilient and verifiable at the threshold level. All characteristics are managed by several authorities, but no single authority has complete control over a single attribute. Our system has a (t;n) secret sharing threshold because in CPABE schemes there is always a secret key used to generate private attribute keys. In typical CPABE schemes, the secret key is the primary key. Master key cannot be accessed by any one authority due to the introduction of secret sharing of threshold (t;n). As long as no less than t permissions are active in the system, PROJECT is not only secure and auditable, but also robust. This study, to our knowledge, is the first to attempt to solve the single bottleneck point for both

security and performance of CPABE access control methods in public cloud storage. " Second, the certifying body is:

It is the certificate authority that sets up the system settings and attribute public keys (PKs) for each attribute in the entire attribute set, and it is this authority that is globally trusted. Legal users and AAs can register with CA by submitting an application with a unique identification and a unique authorization code. In addition, CA sets the parameter t that determines the threshold of AA that is used to generate the user's secret key each time. When it comes to the AA master key and secret key generation, CA is not engaged. As a result, CAs might be anything from government agencies to company divisions tasked with the registration process. The system is built by a certificate authority, which eliminates the need for AA trading system settings. AA synchronisation is avoided thanks to a list of registered users, which is maintained by CA.

3. Give credit where credit is due:

It's the job of attribute authorities to manage attributes and generate unique identifiers for them. Additionally, AAs are in charge of designing and implementing the system, as well as serving as its administrators or managers. It is not possible for each AA to assign a user's private key because the master key is shared by all the AAs, unlike other multi-authority CPABE systems. The master key is shared by all AAs. Using this method, each AA can get a bit of the master key, but when it comes to creating users' secret keys, only each AA must generate the appropriate secret key. Multiple attribute permissions share the primary key. The value of a secret can be earned in the classic threshold (t;n) sharing method once it has been pieced together by a number of participants.

5. RESULTS AND DISCUSSIONS

Fig 2:Home Page

Fig 3: Uploaded File Details

Fig 4: User Request Page

6. CONCLUSION

In this paper, we presented a multiauthority CP-ABE conspiracy to facilitate varied client renunciation and open figure content modification in order to assemble a protected and knowledgeable multi-authority property-based access control plot for information participating in distributed storage frameworks. Decoding keys can be presented without compromising the proposed system's forwarding or reverse security features. In the arbitrary prophet model, we were able to establish the safety of the proposed strategy. Our plan is becoming more and more appealing to people who want to use it in a convenient way

Conflict of interest statement

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

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. Adv. Cryptol.—EUROCRYPT 2005. New York, NY, USA: Springer, 2005,457–473.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[3] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in Proc. IEEE Security Privacy 2007, 2007, pp. 321–334.

[4] M. Perretti, P. Traynor, P. McDaniel, and B. Waters, “Secure attribute-based systems,” in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 99–112.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute-based data sharing with attribute revocation," in Proc. 5th ACM Symp. Inf., Comput. Commun. Security 2010, 2010, pp. 261–270.

[6] S. S. M. Chow, “A framework of multi-authority attribute-based encryption with outsourcing and revocation,” in Proc. 21st ACM Symp. Access Control Models Technol., 2016, pp. 215–226.

[7] J. Hur and D. K. Noh, “Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214–1221, Jul. 2011.

[8] C.-I. Fan, V. S.-M. Huang, and H.-M. Ruan, “Arbitrary-state attribute-based encryption with dynamic membership,” IEEE Trans. Comput., vol. 63, no. 8, pp. 1951–1961, Aug. 2014.

[9] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, “DAC-MACS: Effective data access control for multiauthority cloud storage systems,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 11, pp. 1790–1801, Nov. 2013.

[10] S. Ruj, A. Nayak, and I. Stojmenovic, “DACC: Distributed access control in clouds,” in Proc. 2011 IEEE 10th Int. Conf. Trust, Security Privacy Comput. Commun., 2011, pp. 91–98.

[11] Parvathi, D. S. L., Leelavathi, N., Ravikumar, J. M. S. V., & Sujatha, B. (2020, July). Emotion Analysis Using Deep Learning. In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 593-598). IEEE.

[12] Kumar, J. R., Sujatha, B., &Leelavathi, N. (2021, February). Automatic Vehicle Number Plate Recognition System Using Machine Learning. In IOP Conference Series: Materials Science and Engineering (Vol. 1074, No. 1, p. 012012). IOP Publishing.”