International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Efficient Revocable Multi Authority Based Attribute Encryption

Mr. G. Gopalakrishna *1, **K. Kashi Vishwanath Rao** *2

***1Faculty, *2B.Tech. Student**

Department of Computer Science and Engineering, J.B. Institute of Engineering and Technology, Moinabad Mandal, Hyderabad, Telangana, India

Corresponding Author Email Id: kashikulkarni594@gmail.com

ARTICLEINFO

Article History:

Accepted: 10 April 2023
Published: 30 April 2023

Publication Issue
Volume 10, Issue 2
March-April-2023

Page Number
771-778

ABSTRACT

As is known, attribute-based encryption (ABE) is usually adopted for cloud storage, both for its achievement of fine-grained access control over data, and for its guarantee of data confidentiality. Nevertheless, single-authority attribute-based encryption (SA-ABE) has its obvious drawback in that only one attribute authority can assign the users' attributes, enabling the data to be shared only within the management domain of the attribute authority, while rendering multiple attribute authorities unable to share the data. On the other hand, multi-authority attribute-based encryption (MA-ABE) has its advantages over SA-ABE. It can not only satisfy the need for the fine-grained access control and confidentiality of data, but also make the data shared among different multiple attribute authorities. However, existing MA-ABE schemes are unsuitable for the devices with resources-constraint, because these schemes are all based on expensive bilinear pairing. Moreover, the major challen-Efficient Revocable Multi Authority Attribute based Encryption for cloud storage of MA-ABE scheme is attribute revocation. So far, many solutions in this respect are not efficient enough. In this paper, on the basis of the elliptic curves cryptography, we propose an efficient revocable multi-authority attribute-based encryption (RMA-ABE) scheme for cloud storage. The security analysis indicates that the proposed scheme satisfies indistinguishable under adaptive chosen plaintext attack assuming hardness of the decisional Diffie-Hellman problem. Compared with the other schemes, the proposed scheme gets its advantages in that it is more economical in computation and storage.

Keywords: MA-ABE, SA-ABE, Attribute-Based Encryption

I. INTRODUCTION

Cloud storage is an application pattern of cloud computing to store massive data, so more and more individuals and organizations shift their data from local computers to cloud. However, this new paradigm poses a serious threat to the privacy of their owners, since the data might be accessed and analyzed by the cloud server providers for illegal or monetary purposes.

To solve this problem, people have figured out a variety of approaches. One common way is to resort to the traditional public key encryption technology to encrypt data, but the data owners fail to have fine-grained access to their data flexibly. Accordingly, advanced a new way of encryption, attribute-based encryption (ABE). It used to be considered one of the most promising technologies for cloud storage, since it ensures the data owners to enjoy non interactive and fine-grained control over encrypted data.

Since then, many single-authority attribute-based encryption (SA-ABE) schemes have been put forward. In these schemes, it is required that only one trusted attribute authority administers the attributes and distributes the corresponding secret keys of attributes to the data consumers. This mechanism may not meet the practical requirements in cloud storage, when data consumers' attributes are distributed by multiple different attribute authorities. For example, when a data owner intends to share the data with a targeted data consumer holding the attribute "Professor" from a university and the attribute "Engineer" from a research institution, obviously SA-ABE scheme can not be applied to this scenario. To deal with this problem, many researchers turn to multi-authority attribute-based encryption (MA-ABE), so that secret keys of attributes are issued to data consumers with the corresponding privileges for different attribute authorities respectively. There exists two kinds of multi authority ABE schemes, namely centralized multi-authority ABE and decentralized multi authority ABE, the difference between them is whether the key is distributed by center authority. When the key is distributed by central authority, we can consider it as centralized multiauthority ABE scheme. When the key is distributed by attribute authority, we can consider it as decentralized multi-authority ABE scheme.

From the perspective of practical application, the following challenges should be solved before applying MA-ABE in cloud storage system. One of the major challenges is the highly computational overhead, since the existing MAABE schemes are all based on the expensive bilinear pairing operations, hinders the further development of MA-ABE schemes on the resource constrained devices. The other challenge is the attribute revocable, since multiple data consumers may share the same attribute, and each data consumers may possess multiple different attributes, result in that revocation for anyone attribute may influence the other data consumers in the cloud storage system. Although re encrypting the data is a method to solve this problem, it will generate high computation cost. Another technology is to introduce a timestamp into every attribute, but it is not achieved immediate revocation. This paper involves the construction of an efficient RMAABE scheme for cloud storage. Our main contributes are as follows:

First, based on the elliptic curve cryptography (ECC), an efficient RMA-ABE scheme is proposed for cloud storage, so that bilinear pairing operations will be no longer needed. In the proposed scheme, we use the linear secret sharing schemes (LSSS) to boost the expressiveness of access policy and add version key to attribute to realize immediate attribute revocation.

Second, the security analysis indicates that under the decisional Diffie-Hellman (DDH) assumption, the proposed RMA-ABE scheme achieves the in distinguish ability against the choose plaintext attack (IND-CPA), and satisfies collision resistant and forward secrecy.

Finally, the performance evaluation of the scheme indicates lower the computation cost and lower storage overhead than other schemes.

II. LITERATURE SURVEY

1. A. Sahai and B. Waters Fuzzy identity-based encryption (2005)

We introduce a new type of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we view an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a ciphertext encrypted with an identity, ω ', if and only if the identities ω and ω ' are close to each other as measured by the "set overlap" distance metric. A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the errortolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Additionally, we show that Fuzzy-IBE can be used for a type of application that we term "attribute-based encryption".

In this paper we present two constructions of Fuzzy IBE schemes. Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. We prove the security of our schemes under the Selective-ID security model.

2. V. Goyal, O. Pandey, A. Sahai, and B Waters Attribute-based encryption for finegrained access control of encrypted data (2006)

As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

3. J. Bethencourt and A. Sahai Ciphertext-policy attribute-based encryption IEEE,(2007)

In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call ciphertext-policy attribute-based encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous attribute-based encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as role-based access control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

4. S. Yu, K. Ren, and W. Lou FDAC: Toward fine-grained distributed data access control in wireless sensor networks IEEE,(2011)

Distributed sensor data storage and retrieval have gained increasing popularity in recent years for supporting various applications. While distributed architecture enjoys a more robust and fault-tolerant wireless sensor network (WSN), such architecture also poses a number of security challenges especially when applied in mission-critical applications such as battlefield and e-healthcare. First, as sensor data are stored and maintained by individual sensors and unattended sensors are easily subject to strong attacks such as physical compromise, it is significantly harder to ensure data security. Second, in many mission-critical applications, fine-grained data access control is a must as illegal access to the sensitive data may cause disastrous results and/or be prohibited by the law. Last but not least, sensor nodes usually are resource-constrained, which limits the direct adoption of expensive cryptographic primitives. To address the above challenges, we propose, in this paper, a distributed data access control scheme that is able to enforce fine-grained access control over sensor data and is resilient against strong attacks such as sensor compromise and user colluding. The proposed scheme exploits a novel cryptographic primitive called attribute-based encryption (ABE), tailors, and adapts it for WSNs with respect to both performance and security requirements. The feasibility of the scheme is demonstrated by experiments on real sensor platforms. To our best knowledge, this paper is the first to realize distributed fine-grained data access control for WSNs.

4. K. Yang, X. Jia, and K. Ren Secure and verifiable policy update outsourcing for big data access control in the cloud IEEE,(2015)

Due to the high volume and velocity of big data, it is an effective option to store big data in the cloud, as the cloud has capabilities of storing big data and processing high volume of user access requests. Attribute-based encryption (ABE) is a promising technique to ensure the end-to-end security of big data in the cloud. However, the policy updating has always been a challenging issue when ABE is used to construct access control schemes. A trivial implementation is to let data owners retrieve the data and reencrypt it under the new access policy, and then send it back to the cloud. This method, however, incurs a high communication overhead and heavy computation burden on data owners. In this paper, we propose a novel scheme that enabling efficient access control with dynamic policy updating for big data in the cloud. We focus on developing an outsourced policy updating method for ABE systems. Our method can avoid the transmission of encrypted data and minimize the computation work of data owners, by making use of the previously encrypted data with old access policies. Moreover, we also propose policy updating algorithms for different types of access policies. Finally, we propose an efficient and secure method that allows data owner to check whether the cloud server has updated the ciphertexts correctly. The analysis shows that our policy updating outsourcing scheme is correct, complete, secure and efficient.

III. PROPOSED SYSTEM

1) First, based on the elliptic curve cryptography (ECC), an efficient RMA-ABE scheme is proposed for cloud storage, so that bilinear pairing operations will be no longer needed. In the proposed scheme, we use the linear secret sharing schemes (LSSS) to boost the expressiveness access policy and add version key to attribute to realize immediate attribute revocation.
2) Second, the security analysis indicates that under the decisional Diffie-Hellman (DDH) assumption, the proposed RMA-ABE scheme achieves the indistinguishability against the choose plaintext attack (IND-CPA), and satisfies collision resistant and forward secrecy.

3) Finally, the performance evaluation of the scheme indicates lower the computation cost and lower storage overhead than other schemes.

Advantages:

The proposed system is very effective due to the presence of Attribute revocation which will give more security on cloud data for the data owners.

The system is more effective due to presence of Collision Resistance on outsource data of the cloud users

IV. SOFTWARE AND HARDWARE REQUIREMENTS

4.1 FUNCTIONAL REQUIREMENTS

1. User shall upload the images.
2. The system shall allow the user to upload images.
3. The system shall predict the image and validate it.
4. The system shall provide the correct output
5. System shall allow user to see the suggested products

4.2 NON-FUNCTIONAL REQUIREMENTS

Scalability: System should be able to handle a large number of users. The system is capable enough to work properly.

Speed: The application should be fast. It should not slow down with the increase of number of users. Search functionality should be fast to enable better end-user experience. The system should be quick enough to be able to respond to user actions with a short period of time.

Usability: User interface should be simple and clear to break to understand to any user. At every step of this project user seems to be familiar with the interfaces as they are easy to use.

Availability: The system should be available at every moment to the user. It should be ensured that there should be minimum or no downtime to ensure better user experience for students.

Reliability: The system should be reliable and yield correct results if a user performs any actions. Also, if the farmer uploads a image, the system should ensure that the correct message is delivered to the correct destination without any loss of content.

Testability: The application is tested for validation, uploading images, message structures and works fine.

4.3 HARDWARE REQUIREMENTS:

• RAM	-	4 GB (min)
• Hard Disk	-	20 GB
• Monitor	-	SVGA

4.4 SOFTWARE REQUIREMENTS

• Operating System	- Windows XP
• Coding Language	- Java/J2EE (JSP, Servlet)
• Front End	- J2EE
• Back End	- MySQL

V. STEPS TO DEVELOP PROPOSED PROJECT

Step 1 : Define project objectives and gather the resources.

- What are the services that we are going to provide using this project?
- What are the conditions and restrictions used in this project?
- What are the client needs and demands?
- How many number of support staff do we need after developing the system ?

Step 2 : Design the efficient revocable multi authority using attribute encryption.

Once the website objectives have been confirmed and communicated, there are multiple key factors that needed to be considered when designing the system architecture.

User Interface(UI) : Interface should be clear and easy to understand. Webpage must be eye catchy to attract users. With Django framework in addition we can built it with ease.

Backend : Python and javascript is the coding language we use in backend which connects to the server which helps to send the results obtained from the algorithm to frontend.

DataBase : Database stores information about diseases and users and profiles including their search and feedback.

Step 3 : Implementation – Developing code

After we have clear idea on the architecture of the leaf disease detection system, we will start developing the code. Here, we have 3 stages to develop the code :

Stage 1 : Frontend -HTML

Stage 2 : Backend - Python

Stage 3 : Database - MySQL

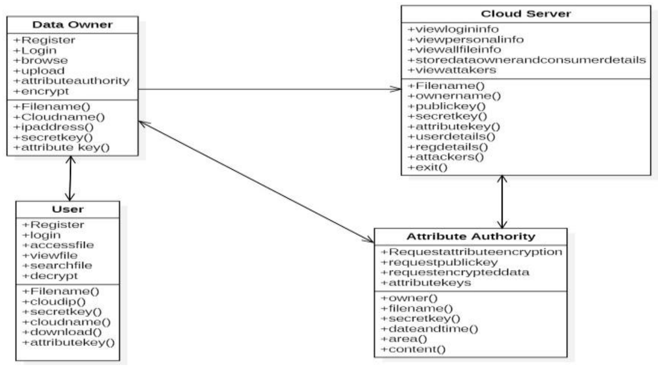
Step 4 : Deployment and Testing

After completing the development of code we need to deploy the project in the compatible system which satisfies all the hardware and software requirement specifications. After deploying successfully we need to check that the software meets the requirements and expectations of the end-users. Code should undergo testing processes like alpha , beta testing, unit testing, integration testing and functional testing to identify mistakes in code developed.

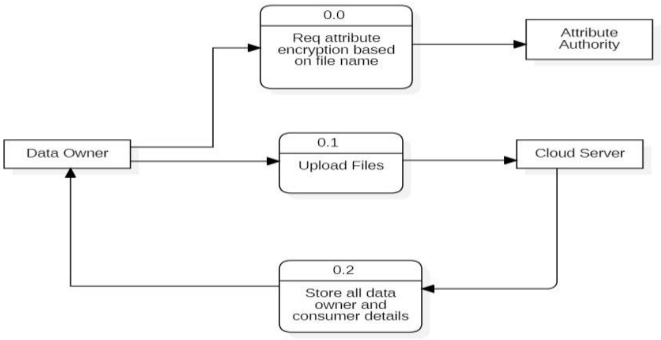
Step 5 : Maintain

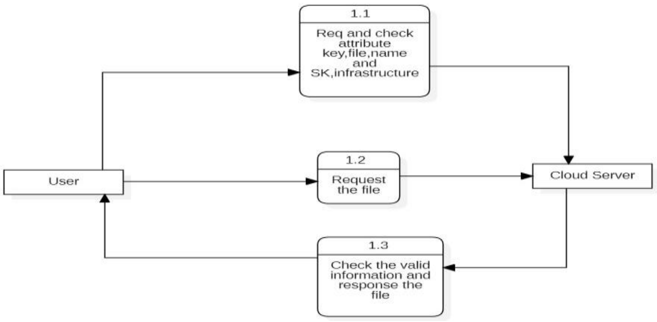
The final step is risk analysis i.e. after testing process every unsuccessful step has some risk which disturbs users accessibility. Our aim is maintain the website with support staff and to make servers available all the time and to analyze risks and update the code to avoid those risks. We need to fix some bugs and features in future as per user feedback. Website should be updated with new features in the future using renewing software models which increases project efficiency and productivity.

VI. CLASS DIAGRAM

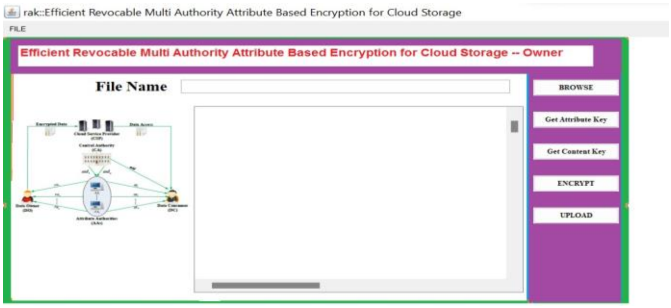


VII. DATA FLOW DIAGRAM


0.0
Req attribute encryption based on file name
Attribute Authority
Data Owner
0.1
Upload Files
Cloud Server
0.2
Store all data owner and consumer details

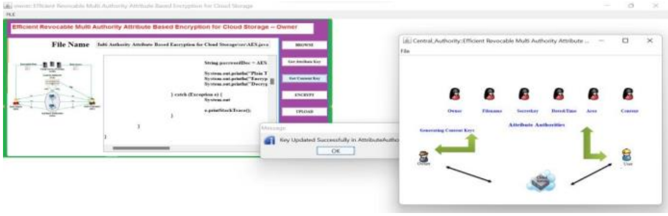

1.1
Req and check attribute key,file,name and SK,infrastructure
User
1.2
Request the file
Cloud Server
1.3
Check the valid information and response the file

EXPECTED OUTCOME

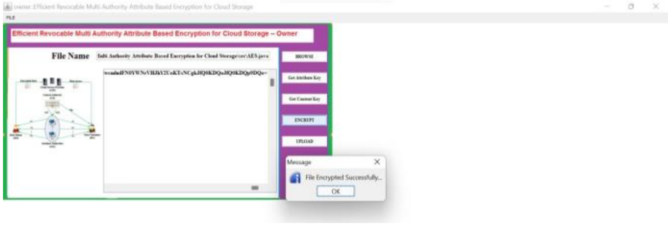

rak::Efficient Revocable Multi Authority Attribute Based Encryption for Cloud Storage

Efficient Revocable Multi Authority Attribute Based Encryption for Cloud Storage -- Owner

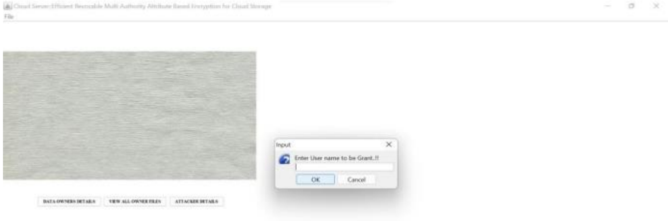
File Name


Efficient Revocable Multi Authority Attribute Based Encryption for Cloud Storage – Owner
File Name
Central_Authority::Efficient Revocable Multi Authority Attribute ...
Attribute Authorities

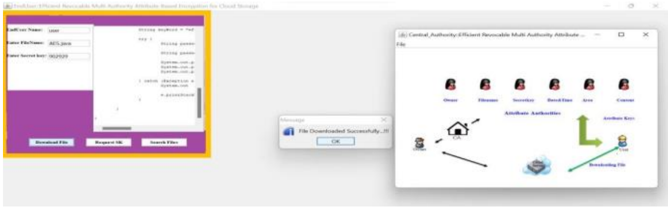
Key Updated Successfully in AttributeAutho...


Efficient Revocable Multi Authority Attribute Based Encryption for Cloud Storage – Owner
File Name
Message
OK

File Encrypted Successfully...



Enter User name to be Grant..!!


Central_Authority::Efficient Revocable Multi Authority Attribute ...
Attribute Authorities
Message
OK

File Downloaded Successfully..!!

VIII. REFERENCES

[1]. P. Mell and T. Grance, “The NIST definition of cloud computing,” Computer Security, pp. 267-269, 2009.

[2]. A. Sahai and B.Waters, “Fuzzy identity-based encryption,” in Advances in Cryptology-EUROCRYPT. Berlin, Heidelberg: Springer, pp. 457-473, Jan.2005.

[3]. V. Goyal, O. Pandey, A. Sahai, and B Waters, “Attribute-based encryption for finegrained access control of encrypted data,” in Proc. of ACM Conference on Computer and Communications Security, ACM, Alexandria, pp.89-98, Jan. 2006.

[4]. J. Bethencourt and A. Sahai, “Ciphertext-policy attribute-based encryption” in Proc. of IEEE Symposium on Security and Privacy, IEEE,California, pp. 321-334, 2007.

[5]. S. Yu, K. Ren, and W. Lou, “FDAC: Toward fine-grained distributed data access control in wireless sensor networks,” IEEE T. Parall. Distr., vol. 22,no. 4, pp. 673-686, Apr. 2011.

[6]. Z. Wan, J. Liu, and R. Deng, “HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing,” IEEE T. Inf. Foren. Sec., vol. 7, no. 2, pp. 743-754, Apr. 2012.

[7]. K. Yang, X. Jia, and K. Ren, “Secure and verifiable policy update outsourcing for big data access control in the cloud,” IEEE T. Parall. Distr.,vol. 26, no. 12, pp. 34613470, Dec. 2015.

[8]. J. Li, X. Lin, Y. Zhang, and J. Han, “KSF-OABE: Outsourced attribute based encryption with keyword search function for cloud storage,” IEEET. Ser. Comput., vol. 10, no. 5, pp. 715-725, Dec. 2017.

[9]. J. Li, X. Lin, Y. Zhang, and J. Han, “User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage,” IEEE Syst. J., vol. 12, no. 2, pp. 17671777, Feb. 2018.

[10]. M. Chase, “Multi-authority attribute based encryption,” in Proc. of Theory of Cryptography Conference. Berlin, Heidelberg: Springer, pp. 515-534, Feb. 2007.

[11]. M. Chase and S. Chow, “Improving privacy and security in multi-authority attribute-based encryption,” in Proc. of ACM Conference on Computer and Communications Security, ACM, NY, pp. 121-130, Jan. 2009.

[12]. A. Lewko and B. Waters, “Decentralizing attribute-based encryption,” in Advances in Cryptology-EUROCRYPT. Berlin, Heidelberg: Springer, pp. 568-588, May 2011.

[13]. Y. Zhang, D. Zheng, Q. Li, J. Li, and H. Li, “Online/offline unbounded multiauthority attribute-based encryption for data sharing in mobile cloud computing,” Security and Communication Networks, vol. 9, no. 16, pp.3688-3702, Aug. 2016. [14] K. Yang, X. Jia, and K Ren, “DAC-MACS: Effective data access control for multiauthority cloud storage

systems," IEEE T. Inf. Foren. Sec., vol. 8, no. 11, pp. 17901801, Nov. 2013.

[14]. J. Li, X. Huang, X. Chen, and Y. Xiang, "Securely outsourcing attribute based encryption with check-ability," IEEE T. Inf. Foren. Sec., vol. 8, no.8, pp. 1343-1354, Aug. 2014.

Cite this article as :

Mr. G. Gopalakrishna, K. Kashi Vishwanath Rao, "Efficient Revocable Multi Authority Based Attribute Encryption", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 2, pp. 771-778, March-April 2023.
Journal URL : https://ijsrset.com/IJSRSET23102110