International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 29 Issue 7 – Aug 2022.

VERSATILE DATA ACCESS CONTROL BASED ON TRUST AND REPUTATION IN CLOUD COMPUTING

P. AJAY[1], M.MOHAMED RAFI [2], Dr.S.SAJITHA BANU [3], M.SABARI RAMACHANDRAN[4]

1. Student, Department of Master of Computer Application. Mohamed Sathak Engineering College. Ramanathapuram, India.
2. Professor, HOD, Department of Master of Computer Application, Mohamed Sathak Engineering College. Ramanathapuram, India.
3. Assistant Professor, Department of Master of Computer Application, Mohamed Sathak Engineering College. Ramanathapuram, India.
4. Assistant Professor, Department of Master of Computer Application, Mohamed Sathak Engineering College. Ramanathapuram, India.

ABSTRACT

Data access control has becoming a challenging issue in cloud storage systems. Some techniques have been proposed to achieve the secure data access control in a semi trusted cloud storage system. Proposed a basic data access control scheme for multiauthority cloud storage system (DAC-MACS) and an extensive data access control scheme (EDAC-MACS). They claimed that the DAC-MACS could achieve efficient decryption and immediate revocation and the EDAC-MACS could also achieve these goals even though non revoked users reveal their Key Update Keys to the revoked user. However, through our cryptanalysis, the revocation security of both schemes cannot be guaranteed. In this project, we first give two attacks on the two schemes. By the first attack, the revoked user can eavesdrop to obtain other users' Key Update Keys to update its Secret Key, and then it can obtain proper Token to decrypt any secret information as a non revoked user. In addition, by the second attack, the revoked user can intercept Ciphertext Update Key to retrieve its ability to decrypt any secret information as a non revoked user. Secondly, we propose a new extensive DAC-MACS scheme (NEDAC-MACS) to withstand the above two attacks so as to guarantee more secure attribute revocation. Then, formal cryptanalysis of NEDAC-MACS is presented to prove the security goals of the scheme. Finally, the performance comparison among NEDAC-MACS and related schemes is given to demonstrate that the performance of NEDAC-MACS is superior to that of DACC, and relatively same as that of DAC-MACS.

KEYWORDS

DAC-MACS (Data Access Control Scheme for Multi Authority Cloud Storage System)

EDAC-MACS (Extensive Data Access Control Scheme)

NEDAC-MACS (New Extensive Data Access Control Schemes)

I. INTRODUCTION

CLOUD computing extends the existing capabilities of Information Technology (IT) since cloud adaptively provides storage and processing services such as SaaS, IaaS, and PaaS that dynamically increase the capacity and add capabilities without investing in new infrastructure or licensing new software . However, the data access control (DAC) issue of cloud computing systems has been

escalated by the surge in attacks such as collusion, wiretapping and distort, so that DAC must be designed with sufficient resistance. DAC issues are mainly related to the security policies provided to the users accessing the uploaded data, and the techniques of DAC must specify their own defined security access policies and the further support of policy updates, based on which each valid user can have access to some particular sets of data whereas invalid users are unauthorized to access the data. One approach to alleviate attacks is to store the outsourcing data in encrypted form. However, due to the normally semitrusted cloud and its arrangement issues of administration rights, cloud-based access control approaches with traditional encryption are no longer applicable to cloud storage systems .Sahai and Waters laid a theoretical foundation for solving above encryption problem by introducing the new concept of attribute-based encryption (ABE) whose prototype is the identity-based encryption (IBE).

II. Existing System

- DAC-MACS could achieve efficient decryption and immediate revocation and the EDAC-MACS could also achieve these goals even though nonrevoked users reveal their Key Update Keys to the revoked user.
- However, through our cryptanalysis, the revocation security of both schemes cannot be guaranteed.

Disadvantages:

- First attack, the revoked user can eavesdrop to obtain other users' Key Update Keys to update its Secret Key, and then it can obtain proper Token to decrypt any secret information as a nonrevoked user.
- In addition, by the second attack, the revoked user can intercept Ciphertext Update Key to retrieve its ability to decrypt any secret information as a nonrevoked user.

PROPOSED SYSTEM

- We propose a new extensive DAC-MACS scheme (NEDAC-MACS) to withstand the above two attacks so as to guarantee more secure attribute revocation.
- Then, formal cryptanalysis of NEDAC-MACS is presented to prove the security goals of the scheme.
- Finally, the performance comparison among NEDAC-MACS and related schemes is given to demonstrate that the performance of NEDAC-MACS is superior to thatof DACC, and relatively same as that of DAC-MACS

III.MODULES DESCRIPTION

1. Global trusted certificate authority:

The CA is a global trusted certificate authority in the system. It sets up the system and accepts the registration of all the users and AAs in the system. The CA is responsible for the distribution of global secret key and global public key for each legal user in the system. However, the CA is not involved in any attribute management and the creation of secret keys that are associated with attributes. For example, the CA can be the Social Security Administration, an independent agency of the United States government. Each user will be issued a Social Security Number (SSN) as its global identity.

2. Attribute Authority:

Every AA is an independent attribute authority that is responsible for issuing, revoking and updating user's attributes according to their role or identity in its domain. In DACMACS, every

attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key for each user associates with their attributes.

3. Cloud Server:

The cloud server stores the owners' data and provides data access service to users. It generates the decryption token of a ciphertext for the user by using the secret keys of the user issued by the AAs. The server also does the ciphertext update when an attribute revocation happens.

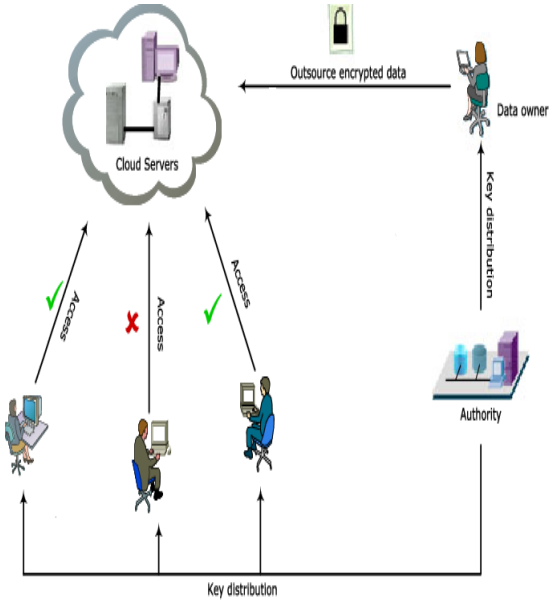
4. Data Owner:

The data owners define the access policies and encrypt the data under the policies before hosting them in the cloud. They do not rely on the server to do the data access control. Instead, the ciphertext can be accessed by all the legal users in the system. But, the access control happens inside the cryptography. That is only when the user's attributes satisfy the access policy defined in the ciphertext, the user can decrypt the ciphertext.

5. User:

Each user is assigned with a global user identity from the CA. Each user can freely get the ciphertexts from the server. To decrypt a ciphertext, each user may submit their secret keys issued by some AAs together with its global public key to the server and ask it to generate an decryption token for some ciphertext. Upon receiving the decryption token, the user can decrypt the ciphertext by using its global secret key. Only when the user's attributes satisfy the access policy defined in the ciphertext, the server can generate the correct decryption token. The secret keys and the global user's public key can be stored on the server; subsequently, the user does not need to submit any secret keys if no secret keys are updated for the further decryption token generation.

IV.SYSTEM ARCHITECTURE



V.SYSTEM TESTING AND IMPLEMENTATION

Software testing is an investigation conducted to provide stakeholders with information about the quality of the product or service under test. Software testing can also provide an objective, independent view of the software to allow the business to appreciate and understand the risks of software implementation. Test techniques include, but are not limited to the process of executing a program or application with the intent of finding software bugs (errors or other defects).

Functional Testing

Functional Testing of the software is conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements. There are five steps that are involved when testing an application for functionality.

Unit Testing

This type of testing is performed by the developers before the setup is handed over to the testing team to formally execute the test cases. Unit testing is performed by the respective developers on the individual units of source code assigned areas. The developers use test data that is separate from the test data of the quality assurance team. The goal of unit testing is to isolate each part of the program and show that individual parts are correct in terms of requirements and functionality.

Integration Testing

The testing of combined parts of an application to determine if they function correctly together is

Integration testing. There are two methods of doing Integration Testing Bottom-up Integration testing and Top- down Integration testing.

Performance Testing

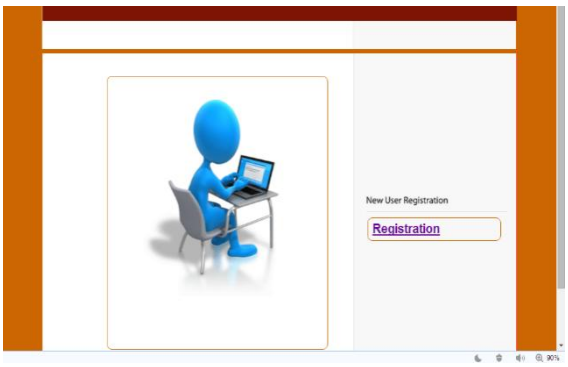
It is mostly used to identify any bottlenecks or performance issues rather than finding the bugs in software. There are different causes which contribute in lowering the performance of software:

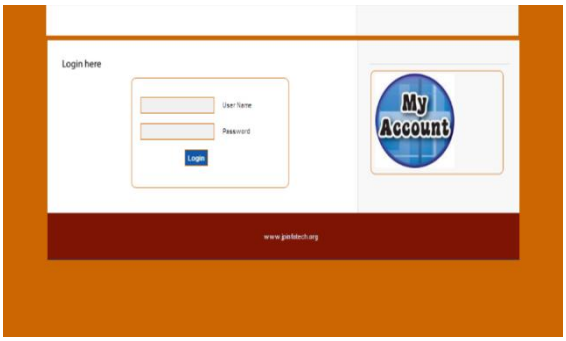
- Network delay.
- Client side processing.
- Database transaction processing.
- Load balancing between servers.
- Data rendering

Regression Testing

Whenever a change in a software application is made it is quite possible that other areas within the application have been affected by this change. To verify that a fixed bug hasn't resulted in another functionality or business rule violation is Regression testing.

VI.WORKING





VII. Conclusion

In this project, I first give two attacks on DAC-MACS and EDAC-MACS for their backward revocation security. Then, a new effective data access control scheme for multi authority cloud storage systems (NEDAC-MACS) is proposed to withstand

the two vulnerabilities in section 3 and thus to enhance the revocation security. NEDACMACS can withstand the two vulnerabilities even though the nonrevoked users reveal their received key update keys to the revoked user. In NEDAC-MACS, the revoked user has no chance to decrypt any objective ciphertext even if it actively eavesdrop to obtain an arbitrary number of nonrevoked users' Key Update Keys KUK or collude with some nonrevoked users or obtain any transmitted information such as Ciphertext Update Keys CUK. Then, formal cryptanalysis of NEDAC-MACS is presented to prove its improved security. Finally, the performance simulation shows the overall storage, computation, and communication overheads of the NEDAC-MACS are superior to that of DACC and relatively same as that of DAC-MACS.

VIII. Future Work

Future change in the environment or processing can be easily adopted by having simple change in coding .It is very user friendly, very high level of security evocation. In future the file access policy can be implemented with Multi Authority based Encryption.

IX.REFERENCES

[1] K. Yang, X. Jia, and K. Ren, "DAC-MACS: Effective data access controlfor multiauthority cloud storage systems," IEEE Trans. Information Forensics and Security, vol. 8, no. 11, pp. 1790-1801, Nov. 2013

[2] Kan Yang and XiaohuaJia, "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage," IEEE Trans. Paralleland Distributed Systems, vol.25, no.7, pp.1735-1744, July 2014

[3] A. Sahai and B. Waters, "Fuzzy identity-based encryption," Proc. EUROCRYPT' 05, pp. 457-473, 2005

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006

[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute Based Encryption," Proc.IEEE Symp. Security& Privacy, pp. 321-334, 2007

[6] J. Bethencourt, A. Sahai, and B. Waters, "Attribute Based Encryption," Proc.IEEE Symp. Security & Privacy, pp.