International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 1, pp: 129-135 www.ijaem.net ISSN: 2395-5252

Security of Data Access Control for Multiauthority Cloud Storage System

Arshi Bano[1], Sayali More[2], Shruti Sukhdeve[3], Bharati Potraje[4], Prof. Sara Sahu[5]
Department of CSE, Ballarpur Institute of Technology (BIT), Ballarpur, India

Date of Submission: 07-06-2020 Date of Acceptance: 22-06-2020

ABSTRACT:
Data access control is an effective way to ensure the data security in the cloud. However, due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Existing access control schemes are no longer applicable to cloud storage systems, because they either produce multiple encrypted copies of the same data or require a fully trusted cloud server.
Ciphertext-Policy Attribute-based Encryption (CP-ABE) is a promising technique for access control of encrypted data. It requires a trusted authority manages all the attributes and distributes keys in the system. In cloud storage systems, there are multiple authorities co-exist and each authority is able to issue attributes independently. However, existing CP-ABE schemes cannot be directly applied to the access control for multi-authority cloud storage systems, due to the inefficiency of decryption and revocation.
Keyword: Access control, attribute revocation, revocation security, CP-ABE, multiauthority cloud

I. INTRODUCTION

DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), an effective and secure data access control scheme with efficient decryption and revocation. Specifically, we construct a new multi-authority CP-ABE scheme with efficient decryption and also design an efficient attribute revocation method that can achieve both forward security and backward security. The analysis and the simulation results show that our DAC-MACS is highly efficient and provably secure under the security model.

Cloud storage is an important service of cloud computing. It allows data owners to host their data in the cloud that provides "24/7/365" data access to the users (data consumers). Data access control is an effective way to ensure the data security in the cloud. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage systems, because it gives the data owner more direct control on access policies and does not require the data owner to distribute keys.

In CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution. The authority can be the registration office in a university, the human resource department in a company, etc. The data owner defines the access policies and encrypts data under the policies. Each user will be issued a secret key according to its attributes. A user can decrypt the ciphertext only when its attributes satisfy the access policies.

II. LITERATURE SURVEY

Data Access Control: A pluralityof data access controlsys-tems(e.g. [2], [3], [7])based on the promising CP-ABEtechniqueareproposed to construct the efficient, secure, fine grained and revocable access schemes. S.Ruj*et al.*(2011) proposed a distributed access control scheme in clouds (DACC) [9] that supported attribute revocation. In DACC, one or more key distribution centers (KDCs) distributed keys to data owners and users. Technically, it requires not only forward security but more indispensable backward security in context of the attribute revocation. However, DACC supported attribute revocation with vulnerable forward security [2].

J.Hur et al.(2011) proposed an attribute-based DAC scheme withefficientrevocation in cloud storage systems, whereas it was designed only for the cloud systems with single trusted authority. In addition, the above two schemes both require data owners to re-encrypt the out-sourced ciphertext after revocation.

Liu et al.(2013) presented a secure multi-owner data sharing scheme called Mona. It is claimed that the scheme can achieve fine-grained access control and secure revocation. However, the scheme will easily suffer from collusion attack by the revoked user and the cloud.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 1, pp: 129-135 www.ijaem.net ISSN: 2395-5252

III. PROPOSED WORK

First construct a new multi-authority CPABE scheme with efficient decryption and design an efficient attribute revocation method for it. Then, we apply them to design an effective access control scheme for multi-authority systems. The main contributions of this work can be summarized as follows.

i) We propose DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), an effective and secure data access control scheme for multi-authority cloud storage systems, which is provably secure in the random oracle model and has better performance than existing schemes.

ii) We construct a new multi-authority CP-ABE scheme with efficient decryption. Specifically, we outsource the main computation of the decryption by using a token-based decryption method.

iii) We also design an efficient immediate attribute revocation method for multi-authority CP-ABE scheme that achieves both forward security and backward security. It is efficient in the sense that it incurs less communication cost and computation cost of the revocation.

IV. METHODOLOGY

In this stage of the project when the theoretical design is turned out into a working system. Thus, it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

This stage involves careful planning, investigation of the existing system and its constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Algorithm used: CP-ABE algorithms

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 attributesaccording 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 theCA. 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 a 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.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 1, pp: 129-135 www.ijaem.net ISSN: 2395-5252

Architecture:

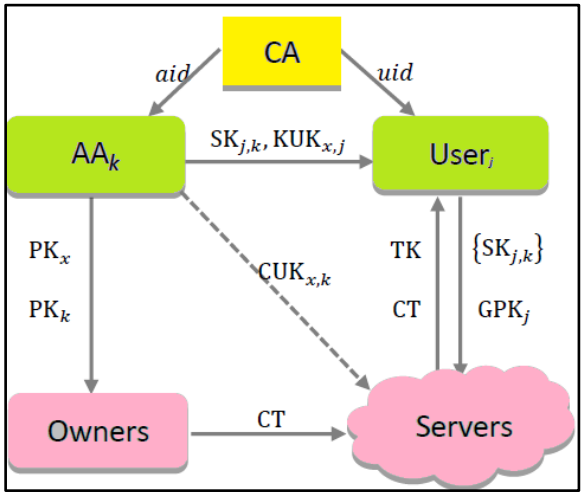
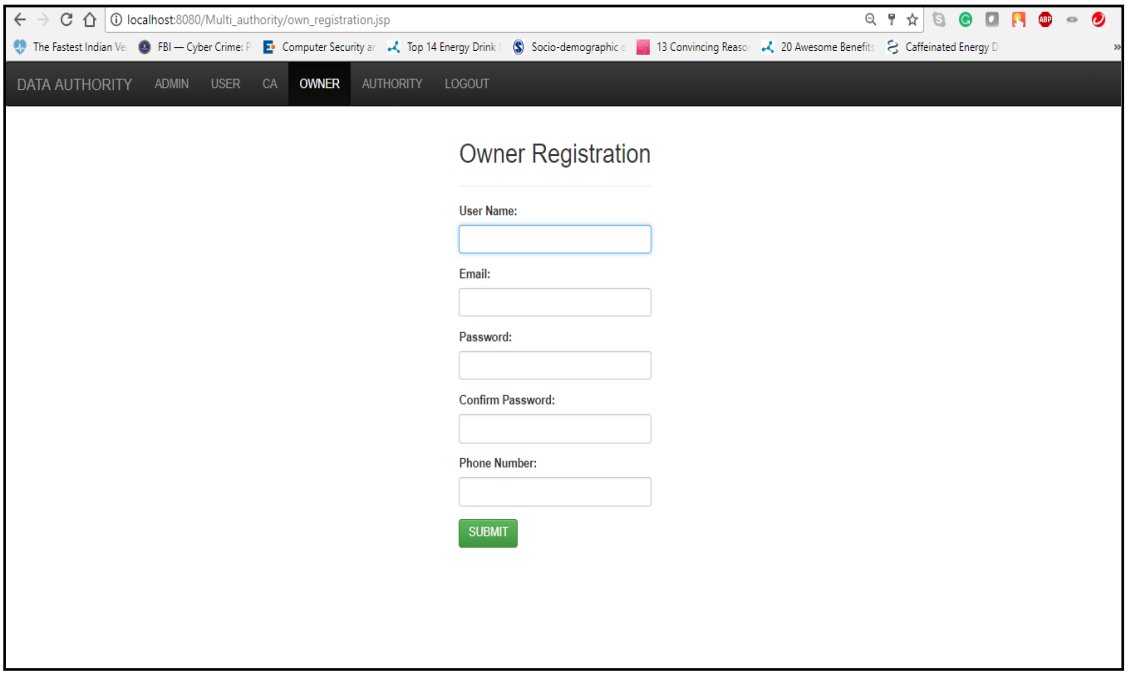


Fig: 1. System Architecture of DAC-MACS

V. RESULT

Figure 2. Login page for the Admin Module
Figure 3. Registration page for Owner Module



International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 1, pp: 129-135 www.ijaem.net ISSN: 2395-5252

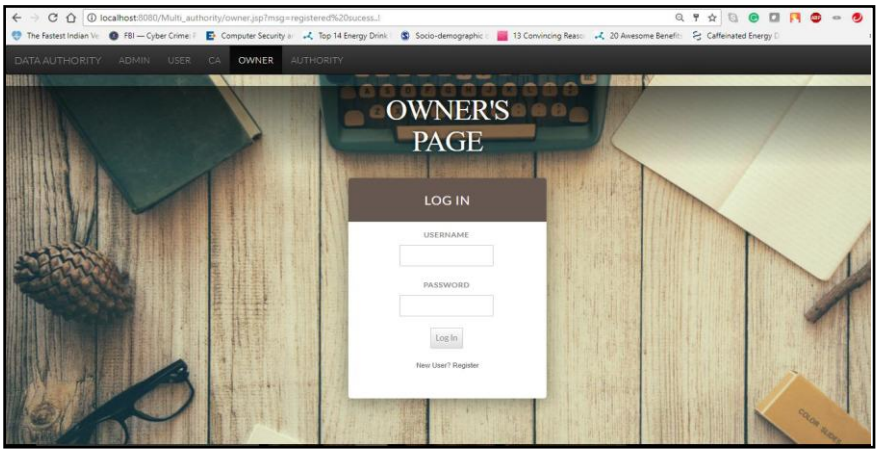


Figure 4. Login page for the Owner Module

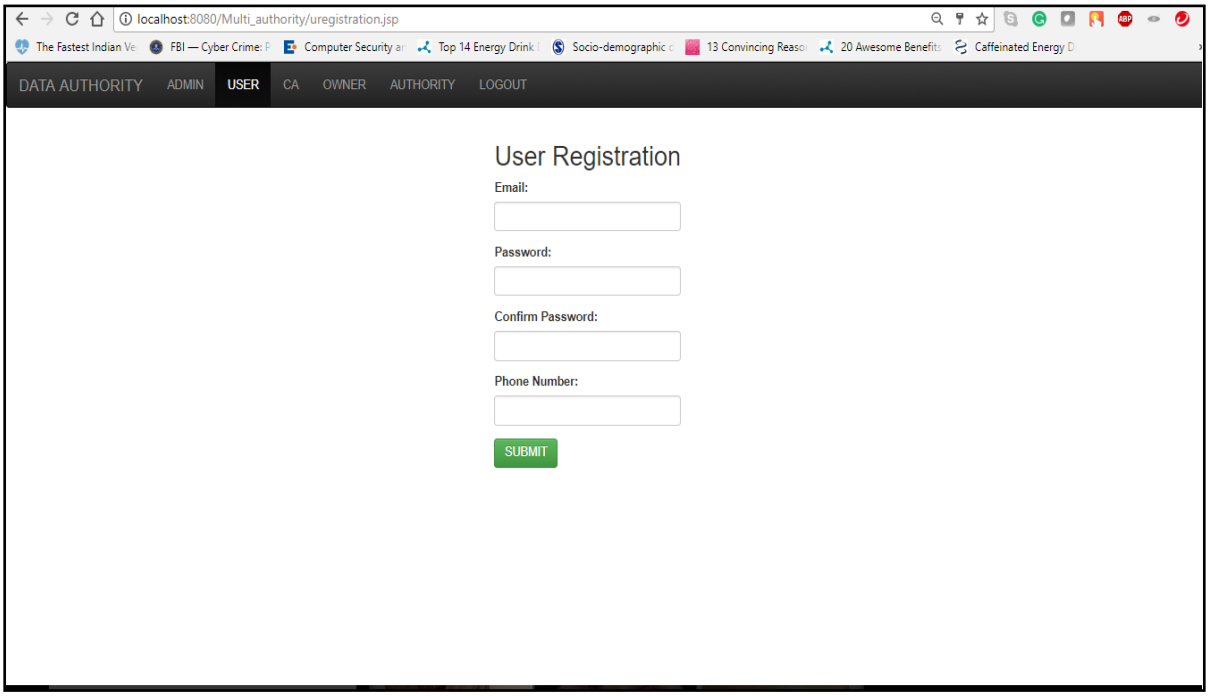


Figure 5. User Registration Page

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 1, pp: 129-135 www.ijaem.net ISSN: 2395-5252

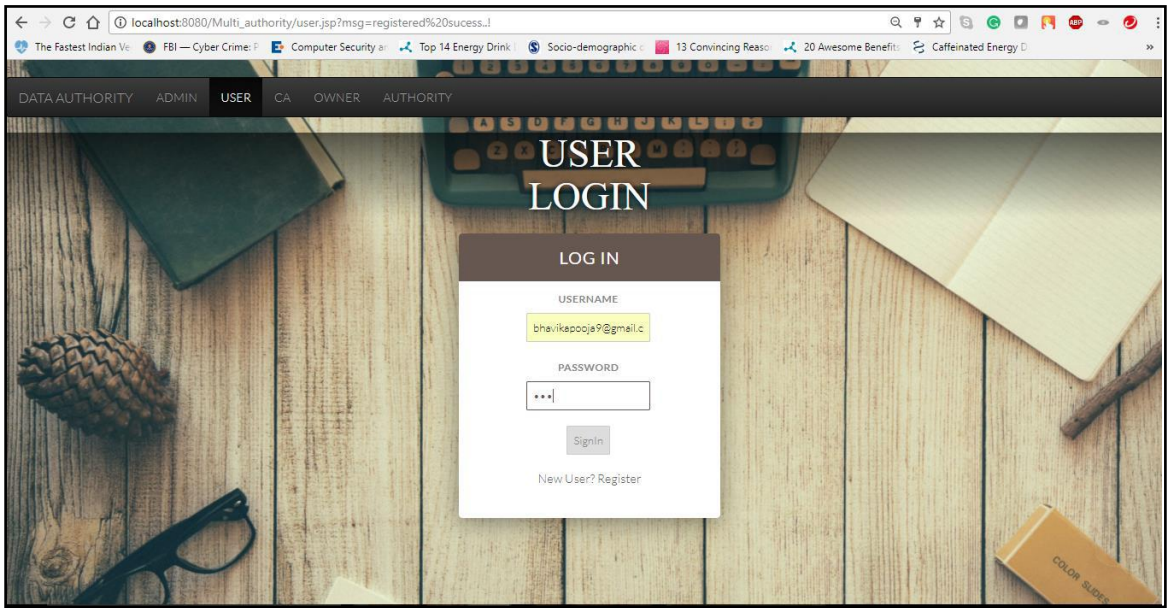


Figure 6. User Login Page

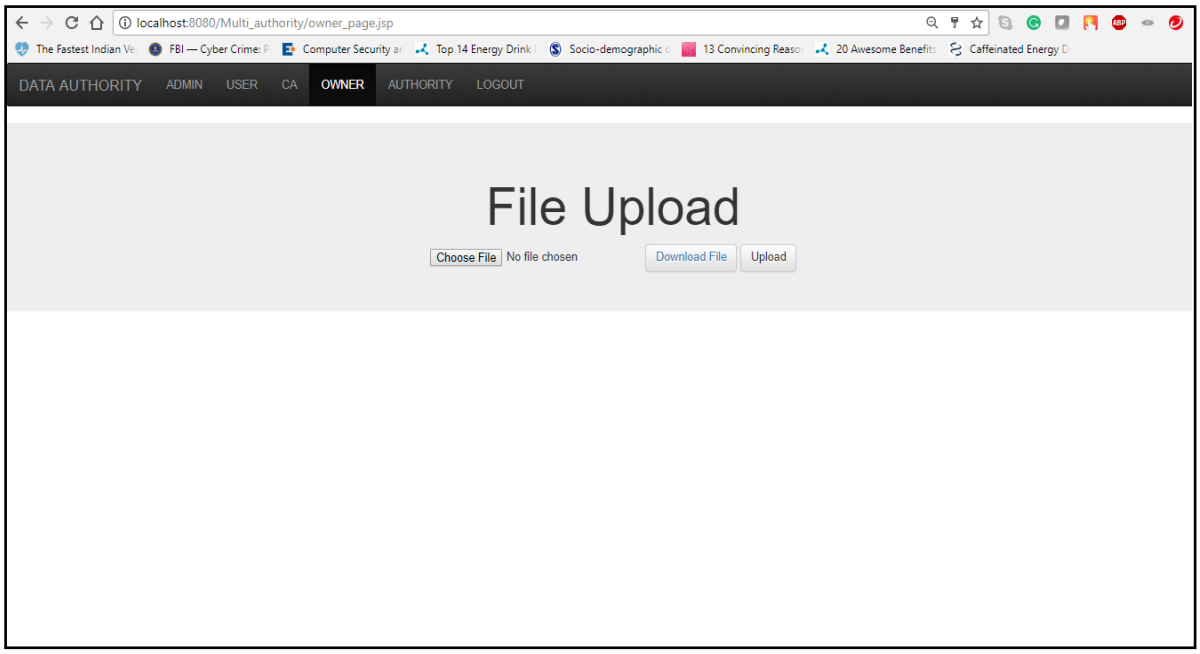


Figure 7. Owner Upload Page

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 1, pp: 129-135 www.ijaem.net ISSN: 2395-5252

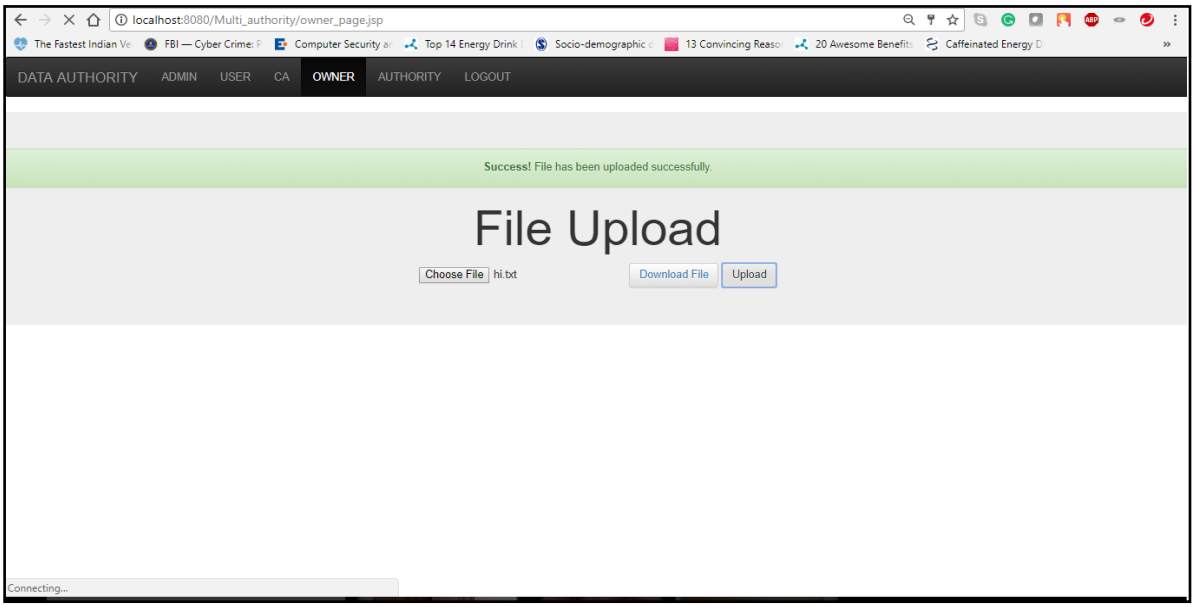


Figure 8. File has been uploaded successfully

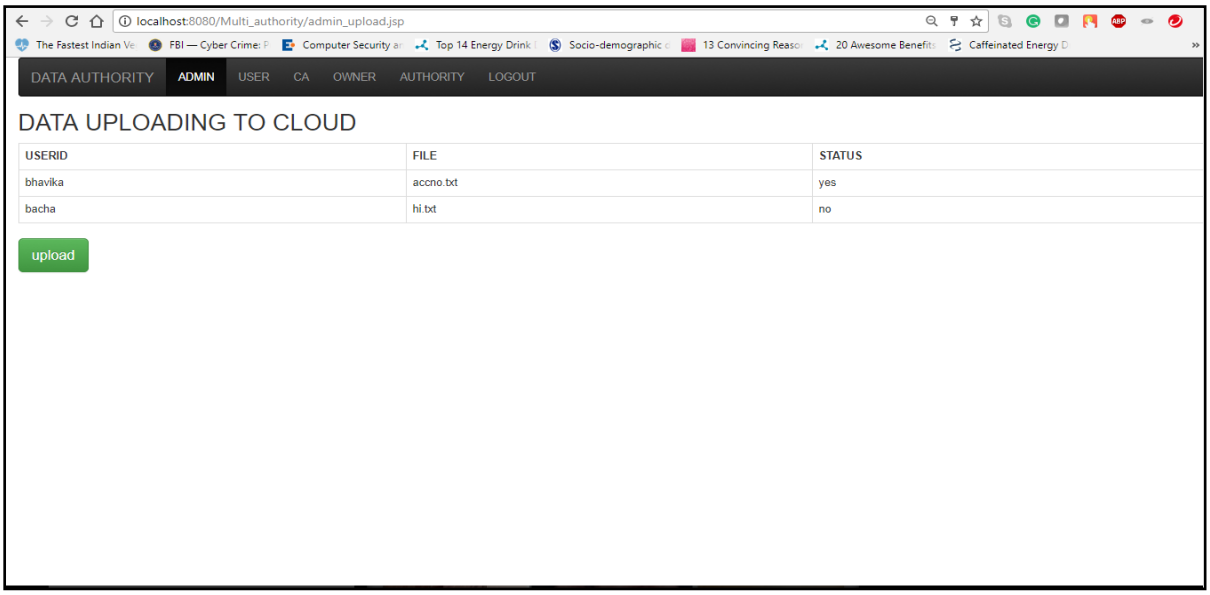


Figure 9. Files Admin uploading to the cloud

V. CONCLUSION

In this paper, we first give two attacks on DAC-MACS and EDAC-MACS for their backward revocation security. Then, a new effective data access control scheme for multiauthority 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.

REFERENCES

[1]. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing,"J. Network and Computer Applications,vol. 34, no. 1, pp. 1-11, Jul. 2010

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

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

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

[5]. 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

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

[7]. R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-Based Encryption with Non-Monotonic Access Structures," Proc. ACM Conf. Computer and Comm.Security, pp. 195-203, 2007

[8]. L. Cheung and C. C. Newport, "Provably secure ciphertext policy ABE,"Proc. ACM Conf. Computer &Communications Security, pp. 456-465, 2007

[9]. S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: distributed access control in clouds," Proc. TrustCom'11, pp. 91-98, IEEE, 2011

Arshi Bano, et. al. "Security of Data Access Control for Multiauthority Cloud Storage System." *International Journal of Advances in Engineering and Management (IJAEM)*, 2(1), 2020, pp. 129-135

International Journal of Advances in Engineering and Management
ISSN: 2395-5252

IJAEM

Volume: 02 Issue: 01 DOI: 10.35629/5252

www.ijaem.net
Email id: ijaem.paper@gmail.com