Multi-Authority Attribute-based Encrypted Access Control System in Cloud Storage

Pranav Sanjay Kute

Computer Department,

Amrutvahini College of Engineering, Sangmner, Ahemednagar, India
Dr. Shrinivas K. Sonkar

Assistant Professor, Computer Department

Amrutvahini College of Engineering, Sangmner, Ahemednagar, India.

ABSTRACT

There Indecent times Data access control has become a Challenging issue for cloud storage systems. There are some techniques that have been applied to achieve in Semi Trusted cloud storage system for achieving the secure data access control.Cloud storage is a very important part of cloud computing which provides services to the owners of the cloud to have their data on the cloud. Cloud Computing is a way without investing in new infrastructure to dynamically increase the capacity and add features.It increases the capabilities of IT services.Cloud Computing has grown in recent years from a promising idea to an integral part of the IT industry. K.Yang et al recently proposed a basic data plan access control system (DAC-MACS) and comprehensive data access control scheme (EDAC-MACS). In what they see demanded that DAC MACS be implemented as soon as possible withdrawal and deletion of active translation. While EDAC MACS and may receive these results even if not revoked users disclose their withdrawals users. in this paper in two processes we give two attacks. During the first attack the retrieved user can listen and get other users key update keys to update. Back that as a non-return user can find you right that as a non revoked user it can obtain proper token and decrypt the secret information. For the second attack the ciphertext update can be intercepted by the user restored to restore his ability to delete any writing label private information as user can be deleted. We have introduced a comprehensive DAC-MACS system to resistance to the above described attacks and assure a more secure withdrawal.
And also we have compared the performance of all the schemes to show that NEDAC- MACS is superior to DACC and almost the same as DACMACS.

Keyword: *DAC-MACS ,EDAC-MACS, NEDAC- MACS and IT*

1 INTRODUCTION

Cloud Computing has increased the current capabilities of the IT industry as cloud provides services for processing such as SaaS, Paas and Iaas adaptively services like this. That dynamically increases the add capabilities and increases capacity without having to invest into new infrastructure or getting into software licensing issues.The issues of in Cloud Computing in DATA Access control have been increased by the increase in attacks such as wiretapping, collusion and distort so that the design of dac should be with a better resistance. The DAC issues are Chiefly related to the security rules given to the user for accessing the uploaded data, security policies must be provided by the DAC techniques and because of which each user can have access to the data if he is authorized and will not have access if he is not authorized. To lessen the attack there is one way that the data that is outsourced can be stored in Encrypted in form. As there are Semi Trusted clouds and the problems with the administrative rights to control cloud-based access including traditional encryption no longer works on the current cloud computing. Sahai and Waters launch a solution-based foundation the above mentioned encryption problems by introducing Attribute based encryption whose Prototype is Identity based encryption. As Abe isb successful there have been many extensive researches on it . V. Goyal et al Proposed a key policy Attribute based system for Fine grained access control. The presented CP-ABE scheme is said to be one of the most fitting techniques in cloud storage systems for data access control. DAC schemes which do not require any data owner can be applied on any type of cloud. There are a Multitude of DAC in cloud storage systems, as can be configured with the file a few DAC schemes that do not require the data owner to perform them, add owner and distribute keys and provide the data owner. But according to to Dolev-Yao’s model[30] Goals related security such as data confidentiality, integrated combat, attack resistance and decryption cannot be fully guaranteed by Dolev-YAo's competent opponents can capture, listen to, and retrieve incomprehensible information from open channels. DACS-MACS and EDAC-MACS[2] due to less secure and open channels the non revoked users can still break through backward revocation whenever they eavesdrop to gain more than 2 valid users.Keys to update their own KEys or when they intercept the cipher update key given from attribute authority to cloud and update their own Secret key.

2 LITERATURE SURVEY

A variety of DACS which is based on the CP ABE technique have been presented to make it effective, fine grained, secure and revocable access schemes. S.Ruj layed down a distributed access control in Clouds that has attribute revocation. IN Those DAAC there are one more key distributed centres keys to users and data owners. Technically it requires more indispensable backward security with the context of backward revocation with forward security. But DAAC supported attributes are vulnerable to backward security.

[2] J Hur et 2011 presented a DAC scheme that has active withdrawals from cloud storage systems, even if they were designed only for cloud systems with a single trusted authority. of them require data Owners to re encrypt the outsourced Cypher text after the revocation.

Liu et al (20130 proposed a Secure multi owner system for data sharing scheme known as mona.It was claimed that this scheme is able to achieved good access control used and safe disposal. But the system often suffers from cloud attacks with retractable users.

K.Yang proposed a data access control system for the multi authority cloud storage systems. Due to assumptions in DAC MACS which both have more secured revocation and secure attribute revocation without revocation by the data owner himself.
DACMACS and EDAC MACS can't still cannot be trusted when the user that is revoke starts to listen in to gain more than two keys for key update.or whenever the user that is revoke updates the Cipher key.

Cloud storage providers can pre presumed to be not dependable and may have false motives like profit to lower the computation and return wrong answers which will not be able to be detected by the valid users.
Recently LAI[23] made modification in the old model of Greens ABE scheme To allow the verifiability of The transformation outsources,

3 OUR CONTRIBUTION

In this paper, attacks on the revocation of DACMACS’s and EDAC-MACS’s cannot be guaranteed using Cryptanalysis. We have proposed a new system name Extensive DAC-MACS scheme is proposed to withstand the above both attacks so as the system can support more secure attribute revocation. In this paper we have constructed two attacks based on the weakness of the revocation security in DACMACS and EDAC MACS. By the first attack there user that is revoked can listen in to get the other user's KEY update , Keys to Update its secret keys. It obtains a perfect token after that a proper token to decrypt any secret information it needs as a non revode user. In addition to the second attack additionally the user that is revoked can intercept the cypher ley to retrieve its ability to decrypt all the secret information as a non revoked user. Further we have proposed an extensive DACMACS scheme Names as MEDAC-MACS, to Survive the above attacks and capable of supporting enough secure attribute revocation.We have modified some algorithms of DACMACS, so that we can perform the vital ciphertext update Communication between AAs and Cloud servers.

4. ANALYSING DAC_MACS and EDAC-MACS:

In this section we have described the attack model and the 2 attack attacks of the EDAC MACS liability and DAC MACS are described in detail.

4.1 Attack Model :

In this paper we have made the Cryptanalysis and layed off a new Extensive Scheme on the basis of Dolev-Yao Model [30] where the Enemy can capture, enter anonymous information and can duplicate any information or message sent = to the communication channel. The only way to increase the security of a sent signal from active or non-active attacks from external and malicious adversaries is to design security protocols .

4.2 Attack 1

There are two phases in attack 1 :i Attack Preparation and implementation during the preparation phase the user that is revoked listens in to gain any two users that are the keys that are not revoked and updated that the phase of of EDAC-MACS this what it looks like right before you fall stumbling around your direction next step we can see it all.Than after that at the implementation phase the revoked user will its secret key by itself and decrypt the CT by being a non revoked user.

4.3 Attack II

The attack two also has two phased the implementation phase and the prep Phase. During the preparation phase the user that is revoked intercepts the Previous CUKxk at the phase of attribute revocation in the EDAC-MACS and EDAC-MACS. Then during the implementation phase the user that is revoked can use the CUCk and can decrypt any secret information as a user that is non revoked.

Adding to it the revoked user can complete all the present related operation by its on as it can learn algorithms CT update and all the corresponding inputs

5. IMPLEMENTATION:

5.1 Objective

To implement a system with multiple attribute authorities to share the load of user validity verification and each of the authorities to manage the whole attribute set individually

To implement a system with CA (Central Authority) who should be chosen one among the AAs, to generate secret keys for legitimacy verified users and the load of user verification is shared by multiple AAs (Attribute Authority)

To withstand the above mentioned attacks and to support a secure attribute revocation. We have proposed a Extensive DAC-MACS scheme, which has been denoted by NEDAC-MACS. We have made modifications in the vulnerability of the DACMACS algorithm so that the vital part of the Cipher text communication between the Cloud and the AA’s have been performed with Magnified security algorithms. Three NEDAC MACS primarily include improvements on EDAC-MACS at the Attribute revocation phase and the Key Generation Phase.

5.1 Security Mechanism:

Same as to DAC MACS, The authorities are only corruptible statically where the adversary queries secret keys under condition that in decrypting the challenge ciphertext secret keys cannot be used. NEDACMACS security model is presented by defining the game between adversary as following step and a challenger.

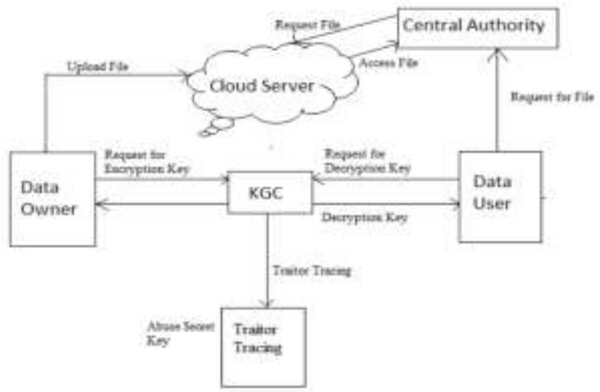
5.2 NEDAC-MACS:

The revoked user will still be able to breach the backward revocation security both in DACMAC island EDAC-MACS because of the open and non secure communication. So we have made modifications in vulnerable algorithms on the EDAC-MACS schemes at the phase of secret key generation. And attribute revocation phase. So the crucial security Strengthen expertise in our NEDAC-MACS programs that can ensure real security objectives of the open and non secure communication. There are two main improvements made: all valid attributes in NEDAC MACS always apply some amount of randomness.

5.2 Architecture.

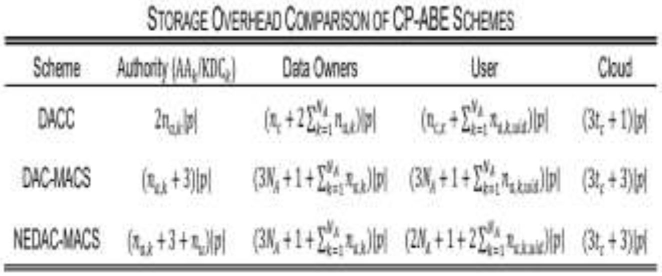
Similar to DAC-MACS, NEDAC-MACS, a high-end data access control for most cloud authorities, has five types of businesses involved: international certification authority (CA), users, cloud servers, data managers, and accounting authorities (AAs). . The security considerations of each business are the same EDAC-MACS. The NEDAC-MACS model framework also consists of five sections: Program Implementation, AAs Privacy Key Performance, Ownership Data Encryption, Data Encryption Users with the help of the cloud, and Attribute Deletion. In the implementation phase of the NEDAC-MACS system, everything compatible algorithms remain the same as in DACMACS. After that in the Secret Key Generation category, in comparison DAC-MACS, the release of the Secret Key algorithm algorithm is converted to NEDAC-MACS by adding a randomly selected number $huid, aid$ piece of AA to calculate SK user-friendly private keys. Currently, part Luid, aid in SK has been changed parallel to L$uid, xaid$linked to responsibility. Thereafter in the data encryption and encryption section, the encryption algorithm by data holder and encryption the algorithm by users is similar to that of DAC-MACS.

After the deregistration, all cryptography algorithms in NEDAC-MACS also remain unchanged without the public key of the returned responsibility involved. Those modified or additional fragments of the DAC-MACS algorithms are as detailed as the two developments below.



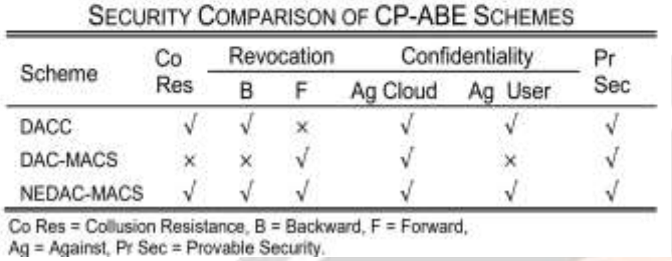
6 RESULTS AND DISCUSSION

To ensure the efficiency of our NEDAC-MACS, performance comparisons were made in the form of a more sophisticated, computerized calculation and high-level communication between DACC's CP-ABE schemes , DAC MACS and our NEDAC-MACS.



STORAGE OVERHEAD COMPARISON OF CP-ABE SCHEMES

Scheme	Authority (AA_k/KDC_k)	Data Owners	User	Cloud
DACC	$2n_{a,k}\|p\|$	$(n_c + 2\sum_{k=1}^{N_A} n_{a,k})\|p\|$	$(n_{c,x} + \sum_{k=1}^{N_A} n_{a,k,uid})\|p\|$	$(3t_c + 1)\|p\|$
DAC-MACS	$(n_{a,k} + 3)\|p\|$	$(3N_A + 1 + \sum_{k=1}^{N_A} n_{a,k})\|p\|$	$(3N_A + 1 + \sum_{k=1}^{N_A} n_{a,k,uid})\|p\|$	$(3t_c + 3)\|p\|$
NEDAC-MACS	$(n_{a,k} + 3 + n_{a})\|p\|$	$(3N_A + 1 + \sum_{k=1}^{N_A} n_{a,k})\|p\|$	$(2N_A + 1 + 2\sum_{k=1}^{N_A} n_{a,k,uid})\|p\|$	$(3t_c + 3)\|p\|$



SECURITY COMPARISON OF CP-ABE SCHEMES

Scheme	Co Res	Revocation		Confidentiality		Pr Sec
		B	F	Ag Cloud	Ag User	
DACC	√	√	×	√	√	√
DAC-MACS	×	×	√	√	×	√
NEDAC-MACS	√	√	√	√	√	√

Co Res = Collusion Resistance, B = Backward, F = Forward,
Ag = Against, Pr Sec = Provable Security.

High communication comparisons were made
between the three strategies regardless of what the common fields say (M, ρ) above the text. Table describes the details of high communication comparisons Following is the comparison of Decryption time of clouds.

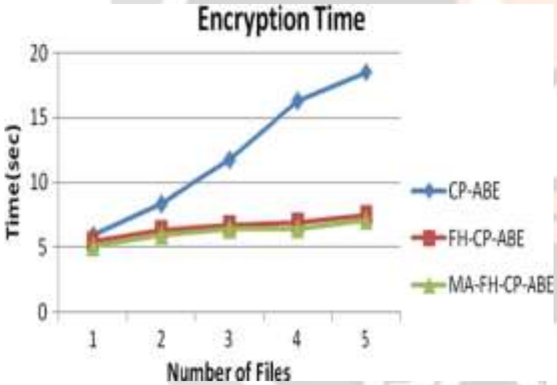


Fig2 : Encryption Time Comparison

Multiple cloud access control data systems (DAC-MACS) is a useful method of verification data security of the cloud storage system. Two the main challenges of current cloud storage systems data extraction and unreliable cloud servers. From the above results we can find out that NEDAC MACS are better than DAC and similar to DAC-MACS.

7 CONCLUSIONS

In the above Paper We have presented two attacks on the DACS and EDAC MACS for their retrospective security. Subsequently, a new multi-cloud data management system (NEDAC-MACS) is proposed to address the two vulnerabilities in Phase 3 and thus improve suspension security. NEDACMACS can withstand two weaknesses though non-retrieved users display their updated keywords returned user keys. In NEDAC-MACS, they have not been withdrawn user does not have the option to delete encrypted text for any purpose ciphertext whether it is listening intently to determine the number of unused users ’KUK Key Recovery Keys or to interact with other users who do not retrieve or obtain any relay information such as Ciphertext Update Keys CUK.Subsequently, NEDAC-MACS cryptanalysis was officially launched to prove its improved security. Finally, performance simulation indicates complete maintenance, calculation, and the top links of NEDAC-MACS are higher than that of the DACC and almost identical to that of DAC-MACS.

8 ACKNOWLEDGMENTS

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally I wish to thank all our friends and well-wishers who supported us in completing this paper successfully. I am especially grateful to my guide for his time to time support, very much needed, valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

.