IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 11-15
www.iosrjournals.org

Multi attribute authority Cipher text Attribute Based Encryption approach with multi Central Authority

Miss S.M.Mahalle Dr.V.M.Thakare
SGBAU, Amravati India.

Abstract: *Data access Control is a mechanism which defines a set of conditions or criteria to access the system and its resources. It is an effective way to ensure data security in the cloud. This paper is focused on efficient data access control schemes for Multiauthority Cloud Storage Systems, DIFC with authorization condition, outsourced policy updating method for big data access control, and also explain ID-based ring signature with forward security. A revocable multiauthority CP-ABE scheme is no longer applicable to cloud storage system. Because in this method single Central authority (CA) is used. Which is responsible for providing id to user, Owner & Attribute Authority. Here this single CA can easily decrypt any Cipher Text on to cloud. So to overcome such a drawback this paper proposed a new multi CA Multi AA CPABE scheme with efficient revocation and decryption. This proposed method serves all the needs of effective access control mechanism for Multiauthority Cloud Storage Systems.*

Keywords— *Data access control, Multiauhority cloud, CP-ABE, outsourcing, policy updating, ABE, DIFC-AC.*

I. INTRODUCTION

In cloud computing Data access Control is an effective way to ensure data security. Data access control enforces security policies by gating access to processes and services within a computing solution via identification, authentication, and authorization.Traditional access control technologies in extremely dynamic cloud computing system provide no autonomic authorization and access control for the users on their data in remote cloud. Once data is stored to the cloud, the user transfers the control to the cloud services providers and cloud hardware. So, data protection is most primary concerns and major challenges of users in cloud computing. Access control model such as Decentralized Information Flow Control with Authorization Condition (DIFC-AC) overcome the problem of the data protection in cloud is how the users can control their data in another control domain. Data Access Control for Multiauthority Cloud Storage is an effective and secure data access control scheme for multiauthority cloud storage systems. In DAC-MACS scheme CA (certification authority) is not responsible for any attribute management and the creation of secret keys.

This paper discusses various methods such as data access control scheme (DAC-MACS), a revocable multiauthority CP-ABE scheme, Decentralized information flow control with authorization condition (DIFC-AC), outsourced policy updating method for ABE system, and ID-based ring signature with forward security. The proposed multi CA Multi AA CPABE scheme for Multiauthority Cloud Storage Systems has good performance and provide high Scalability, Efficiency and Security than DAC-MAC.

II. BACKGROUND

The study on data access control discusses the most relevant access control techniques developed in recent years. Existing Cipher text-policy attribute-based encryption (CP-ABE) technique cannot be directly applied to construct a data access control scheme for multiauthority cloud storage systems, due to the inefficiency of decryption and revocation. So DAC-MAC access control for multiauthority cloud storage is an effective and secure data access control scheme with efficient decryption [1]

In revocable multiauthority CP-ABE scheme the revoked user cannot decrypt any new ciphertext that requires the revoked attribute to decrypt and also achieves forward security. This scheme prevents the server from getting the content of the cloud data by using the proxy encryption method. And it incurs less storage overhead [2].

Ring signature is a useful candidate to construct an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. The costly certificate verification becomes a bottleneck for this solution to be scalable. Identity-based (ID-based) ring signature eliminates the process of certificate verification [3].

Decentralized Information Flow Control with Authorization Condition (DIFC-AC) overcome the problem of the data protection in cloud is how the users can control their data in another control domain. This new access control model annotates the data by security labels with authorization condition which express the confidentiality and integrity demands of the users, and the data access is arbitrated by intercepting IPC-relevant system calls. Thereby, the controls on the data are reached to the cloud [4].

When the data owner wants to change the access policy, it need to transfer the data back to the local site from the cloud, re-encrypt the data under the new access policy, and then move it back to the cloud server. This method incurs a high communication overhead and heavy computation burden on data owners. So there is a need to develop a new method to outsource the task of policy updating to cloud server [5].

This paper introduces various methods such as Extensive data access control scheme (EDAC-MACS), a revocable multiauthority CP-ABE scheme, Decentralized information flow control with authorization condition (DIFC-AC), outsourced policy updating method for ABE system, and ID-based ring signature with forward security and these are organizes as follows. **Section I** Introduction. **Section II** discusses Background. **Section III** discusses previous work. **Section IV** discusses existing methodologies. **Section V** discusses attributes and parameters and how these are affected on data access control. **Section VI** proposed method and outcome result possible. Finally **section VII** Conclude this review paper.

III. PREVIOUS WORK DONE

In research literature, to improved data access control increase efficiency using recent techniques [1][2][3][4][5].

In DAC-MACS, the attribute revocation is controlled and enforced by each independently, but the ciphertexts are updated by the semitrusted server, which can reduce the workload on owners. For the security of attribute revocation, DAC-MACS can achieve both forward security and backward security [1]. An expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems is a revocable CP-ABE scheme where there are multiple authorities co-exist and each authority is able to issue attributes independently [2]. The security of ID-based ring signature can be enhances by providing forward security: If a secret key of any user has been compromised, all previous generated signatures that include this user still remain valid. This property is very important to any large scale data sharing system, as it is impossible to ask all data owners to reauthenticate their data even if a secret key of one single user has been compromised [3]. DIFC-AC expands the security label of DIFC with authorization condition and arbitrates access at standard operating system (OS) abstract. It controls the uncontrollable channel strictly, where only minimum security data can be transmitted. So, the enough security provided by data flow [4]

A scheme that enabling efficient access control with dynamic policy updating for big data in the cloud and focus on developing an outsourced policy updating method for ABE systems. Outsourced policy updating 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 [5].

IV. EXISTING METHODOLOGIES

There are different methodologies that are implemented for data access control i.e Decentralized information flow control with authorization condition (DIFC-AC), outsourced policy updating method for ABE system, DAC-MACS, a revocable multiauthority CP-ABE scheme, and ID-based ring signature with forward security.

Data Access Control for Multiauthority Cloud Storage is an effective and secure data access control scheme for multiauthority cloud storage systems. In DAC-MACS scheme CA (certification authority) is not responsible for any attribute management and the creation of secret keys. DAC-MACS requires all the AAs(attribute authorities) to generate their own public keys which can be used to encrypt data together with the global public parameters, instead of only using the system unique public key for data encryption. This solves the security drawback i.e., it prevents the CA from decrypting the ciphertexts [1].

In Revocable multi-authority CP-ABE scheme the ciphertexts that associated with the revoked attribute needs to be updated and both the key and the ciphertext can be updated by using the same update key, instead of requiring the owner to generate an update information for each ciphertext, such that owners are not required to store each random number generated during the encryption. This scheme prevents the server from getting the content of the cloud data by using the proxy encryption method [2].

Forward secure ID-based ring signature scheme is an essential tool for building cost-effective authentic and anonymous data sharing system. It is secure in random oracle model, under the standard RSA assumption. The elimination of the costly certificate verification process makes it scalable and especially suitable for big data analytic environment. This scheme is very efficient and does not require any pairing operations. In this the size of user secret key is just one integer, while the key update process only requires an exponentiation [3].

The decentralized information flow control model with authorization condition (DIFC-AC) annotates the data by security labels with authorization condition. It provides the confidentiality and integrity demands of the users, and the data access is arbitrated by intercepting IPC-relevant system calls. Thereby, the controls on the data are reached to the cloud. DIFC-AC is stricter than other DIFCs in the authorizations, but is more suitable for the low-trust cloud [4].

Policy updating outsourcing is a correct, complete, secure, efficient and verifiable method. It solves the policy updating problems in ABE scheme. In this scheme instead of retrieving and re-encrypting the data, data owners only send policy updating queries to cloud server, and cloud server update the policies of encrypted data directly, means the cloud server does not need to decrypt the data before/during the policy updating [5].

Following figure shows the data access control system for multi-authority cloud storage, as described in Fig. 1. There are five types of entities in the system these are a certificate authority (CA), attribute authorities (AAs), data owners, the cloud server and data consumers (users).

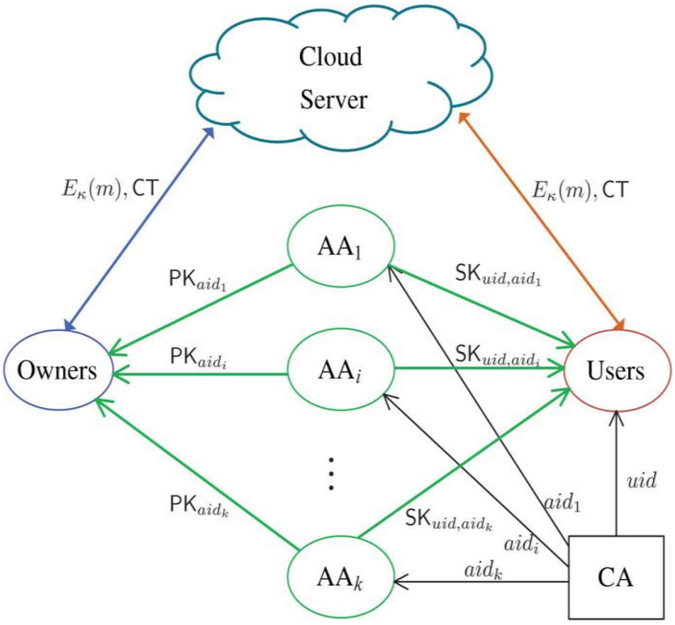

Fig.1: Model of data access control in multiauthority cloud storage.

V. ANALYSIS AND DISCUSSION

The storage overhead on each user in DAC-MACS comes from the global secret key issued by the CA and the secret keys issued by all the AAs. It has less computation cost for the decryption on the user and less communication cost for the revocation. The backward security in DAC-MACS will no longer be guaranteed [1].

Multi-authority revocable CPABE method is efficient in the sense that it incurs less communication cost and computation cost, and is secure in the sense that it can achieve both backward security and forward security. The storage overhead on each AA in this scheme is also linear to the number of users user's in the system. In this the forward security cannot be guaranteed [2].

Forward secure ID-based ring signature provides unconditional anonymity and can be proven forward secure unforgeable in the random oracle model. In this the size of user secret key is just one integer, while the key update process only requires an exponentiation. This scheme will be very useful in many other practical applications, especially to those require user privacy and authentication, such as ad-hoc network, e-commerce activities and smart grid [3].

DIFC-AC's greatest advantage is that authorization condition is used to substitute code command, thus ease the software development and using of existing software. DIFC-AC's security relies on the security of all involved Monitors, Porters, kernels, hardware, data flow, authorization and access control. [4].

Dynamic policy access control scheme is secure in the generic bilinear group model and random oracle model. Policy update outsourcing method can guarantee data owners cannot use their secret keys to decrypt any ciphertexts encrypted by other data owners. In this method, the data owner only needs to send the update keys to the cloud server, instead of the whole encrypted big data. Therefore, this method reduces the communication cost during the policy updating and it incur less computation cost on data owners, as well as less total computation cost [5].

IFC Techniques	Advantages	Disadvantages
DAC-MACS	1) It is secure in the random oracle model. 2) It has less computation cost for the decryption on the user and less communication cost for the revocation	The revocation mechanism in DAC-MACS doesn't satisfy the property of backward security, and brings security vulnerability.
Multi-authority revocable CPABE method	1) It incurs less communication cost and computation cost. 2 it can achieve both backward security and forward security.	The cloud server in this method is required to be semi-trusted otherwise the server will not update the ciphertexts correctly.
Forward secure ID-based ring signature scheme	1) It provides unconditional anonymity and can be proven forward secure unforgeable in the random oracle model. 2) This scheme is very efficient and does not require any pairing operations	Adding forward security on ring signatures is very difficult.
DIFC-AC	1) It provides users confidentiality, integrity and controllability of their data. 2) DIFC-AC is stricter than other DIFCs in the authorizations, but is more suitable for the low trust cloud.	Authorization and access control by using DIFC-AC are secure if and only if the labels are secure and the Monitor can exactly control all data access by the labels and all foresaid formulas.
policy updating outsourcing method:	1) It is correct, complete, secure and efficient. 2) In this the heavy communication overhead of the data retrieval can be eliminated and the computation cost on data owners can also be reduced	Implementation may be complex than other ABE schemes. .

TABLE : Comparisons between DAC-MACS, Multi-authority revocable CPABE, Forward secure ID-based ring signature, DIFC-AC, policy updating outsourcing.

VI. PROPOSED METHODOLOGY

Many access control schemes for Multiauthority Cloud Storage Systems have been used, such as DAC-MACs method and revocable multiauthority CP-ABE method, each of which has its own special characteristics. DAC-MAC is secure in the random oracle model and has better performance. It has less computation cost for the decryption on the user and less communication cost for the revocation. Multiauthority CP-ABE support both efficient decryption and revocation. In revocable multiauthority CP-ABE scheme the ciphertexts that associated with the revoked attribute needs to be updated and both the key and the ciphertext can be updated by using the same update key, instead of requiring the owner to generate an update information for each ciphertext, such that owners are not required to store each random number generated during the encryption. But These Multiauthority access control techniques are no longer applicable to cloud storage system .Because single Central authority(CA) is used in both thods. Which is responsible for providing id to user & Owner & Attribute Authority. Because of that this single CA can easily decrypt any Cipher Text on to cloud. So to overcome such a drawback this paper proposed a new multi CA Multi AA CPABE scheme with efficient revocation and decryption, here the single CA replace to multi CA with multi AA.

Following figure shows a simplified rule based distributed Information Flow Control.

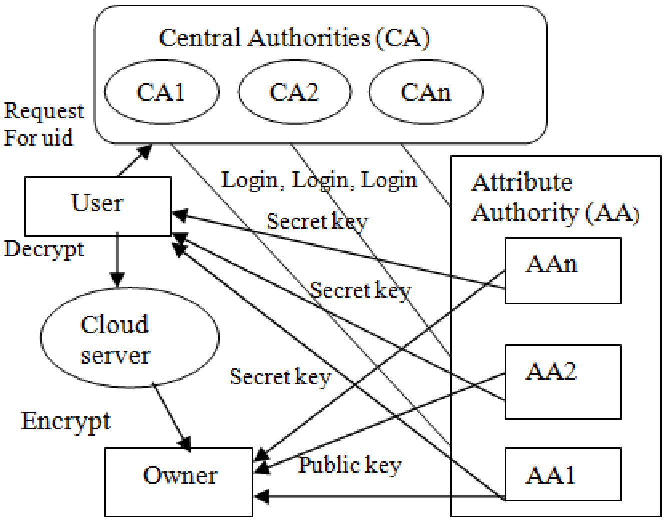

Fig.2: System model for MA-ABE with multi CAs

OUTCOME AND POSSIBLE RESULT

The proposed method provide fine grained, effective and secure access control for trusted cloud storage system. This scheme has good performance than DAC MAC & efficient, expressive DAC MAC by Ken Yang scheme. The RSA algorithm is used in proposed scheme for encryption and decryption purpose, and as compared to existing scheme this system require less time for encryption and decryption. It provides high Scalability, Efficiency, and Security. The multi CA Multi AA CPABE scheme reduce the cost for accessing the information as it can be accessed from anywhere and any time. This system can provide data integrity.

VII. CONCLUSION

This paper focused on some Multiauthority access control schemes such as DAC-MACS scheme and a revocable multiauthority CP-ABE scheme. However, the outputs of DAC-MACS and a revocable multiauthority CP-ABE scheme can be regressed because in both methods single Central authority (CA) is used. This single CA can easily decrypt any Cipher Text on to cloud. The proposed method multi CA Multi AA CPABE can overcome such a drawback by replacing the single CA to multi CA. Main goal of this scheme is to provide security against decrypting every cipher text by single central authority in Multi Attribute Authority -Attribute Based Encryption with single Central Authority system. In this different AA are managed by central authority according to their attribute domain. And no authority can independently decrypt any Cipher Text. So proposed scheme can achieve more security as compared to Multi Attribute Authority Attribute Based Encryption single CA.

FUTURE SCOPE:

From Observation, the multi CA Multi AA CPABE scheme is more suitable for Multiauthority Cloud Storage Systems. Future planned can be tried to apply proposed scheme into applications, such as any remote storage systems, online social networks etc.

REFERENCES

[1]. Kan yang and Xiaohua Jia, “DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems”, *IEEE Transactions on Information forensics and security*, VOL. 8, NO. 11, PP. 1790-1801, NOVEMBER 2013.

[2]. Kan yang and Xiaohua Jia , “Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage”, *IEEE Transactions on parallel and distributed system*, VOL. 25, NO. 7, PP. 1735-1744, JULY 2014.

[3]. Xinyi Huang and Joseph K, “Cost-Effective Authentic and Anonymous Data Sharing with Forward Security”, *IEEE Transactions on computers*, VOL. 64, NO.4, PP. 971-983, APRIL 2015.

[4]. Ye Jianwei and Xu Jie, “Protecting Cloud Data Using the Decentralized Information Flow Control with Authorization Condition”, *IEEE Transactions on cloud computing*, VOL. 5,NO.3, PP. 230-234, JUNE 2015.

[5]. Kan yang and Xiaohua Jia , “Secure and Verifiable Policy Update Outsourcing for Big Data Access Control in the Cloud”, *IEEE Transactions on parallel and distributed system*, Vol. 26, NO. 12, PP. 3461-143470, DECEMBER 2015.