International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 08
July 2019

cryptcloud+: Expressive, Efficient and Revocable Data Access Control for Cloud Storage

Suresh Kumar Potnuru#1, Raja Jacob Chidipi#2

1Student, Computer Science and Engineering, NOVA College of Engineering and Technology, Vegavaram(V), Jangareddigudem(M) West Godavari(D) Andhra Pradesh

2Guide, Associate Professor, Computer Science and Engineering, NOVA College of Engineering and Technology, Vegavaram(V), Jangareddigudem(M) West Godavari(D) Andhra Pradesh

Abstract – Cipher text-Policy Attribute-Based Encryption(CP-ABE) is viewed as a standout amongst the most encouraging systems that might be utilized to secure the assurance of the service. Be that as it may ,the utilization of CP-ABE may yield an unavoidable security rupture which is known as the misuse of access credential (i.e. decryption right). In this paper, we examine the two primary instances of access credential abuse: one is on the semi-trusted authority side, and the other is in favour of cloud client. To relieve the misuse, we propose revocable CP-ABE based cloud storage framework with explicit revoking, timed data accessing and multiple auditing abilityreferred asCloud. Additionally, present the security investigation and further show the utility of framework.

I. INTRODUCTION

CLOUD storage is an important service of cloud computing, which offers services for data owners to host their data in the cloud. This new paradigm of data hosting and data access services introduces a great challenge to data access control. Because the cloud server cannot be fully trusted by data owners, they can no longer rely on servers to do access control. Cipher text-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. 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 according to the policies. Each user will be issued a secret key reflecting its attributes. A user can decrypt the data only when its attributes satisfy the access policies.

In the ciphertext-policy attribute-based encryption, every client's private key (decoding key) is fixed to a set of properties that client's consents. At the point when a ciphertext is encoded, set of qualities is assigned for the encryption, and just clients attached to the significant qualities can

decrypt the ciphertext. In a few cloud frameworks a client should just be ready to

access information if a client has a specific attributes or properties. As of now, the main technique for implementing such arrangements is to utilize a confided in server to store the information and intervene to get control. Be that as it may, if any server putting away the information is undermined, at that point the secrecy of the information will be undermined. In this paper we present a framework for acknowledging complex access control on scrambled information that we call Ciphertext-Policy Property Based Encryption [1].

Any information that is stored in cloud if leaked, could result in arange of consequences for the association and people. The existing CP-ABE based[1] schemeenables us to keep security breach from outside attacker and also an insider of the association who commits the "crimes" of redistributingthe decryption rights and the circulation of understudy data in plain arrangement for illicit financial picks ups. At the same time, it can also ensure that semi-trusted authority won't (re-)distribute the created access credentials to others by proposing CryptCloud+, which provided an accountable authority and revocable CP-ABE based cloud storage system. In any case, one trying issue in taking care of client disavowal in cloud storage is that a revoked client may in any case will still have the capacity to unscramble an old ciphertext they were approved to access before being revoked. To address this issue, the ciphertext put away in the cloud storage ought to be updated, preferably by the (untrusted) cloud server. Also it lacked timed data accessing control which would provide a substantial level of security.

CP-ABE (Ciphertext- Policy Attribute-Based Encryption) is increasingly suitable, as it empowers the information proprietor to more unreservedly characterize the entrance control strategy. Additionally, because the entrance control arrangement itself may release basic data, endeavors have been made [to shroud the entrance control strategy by blinding the qualities inside it].

bank data put away in cloud could result in ramifications for the bank and people (e.g., suit, litigations, and criminal charges). The CP-ABE may enable us to avoid security rupture from outside malicious users. However, when authority misuses the access credentials it is difficult to trace. The proposed system tries to overcome the disadvantage by tracing the malicious inside attackers. The CPABE provides practical solution thus by tracing and evaluating attackers.

II. LITERATURE SURVEY

Two diverse key offers for every one of the clients are produced, with the client just getting one offer. The ownership of a solitary offer of a key enables the SeDaSC philosophy to counter the insider dangers. The SeDaSC approach is material to customary and versatile distributed computing situations. The SeDaSC philosophy works with three substances as pursues: 1) clients; 2) a cryptographic server (CS); and 3) the cloud.

For secure information sharing, SeDaSC does not use the idea of re-encryption with numerous keys. The encryption is finished with a solitary symmetric key. Be that as it

may, the approved clients are conceded access based on ownership of the key offer and the run of the mill validation and approval wonder. The ACL records the approved clients with their accreditations and relating CS key offers. After confirmation, the client offer of the key is utilized, alongside the CS share, to create K. As the client share is just controlled by a legitimate client, just a substantial client can prompt effective encryption/decoding of the information.

Re-appropriated ABE (OABE) with fine-grained get to control framework can to a great extent decrease the calculation cost for clients who need to get to scrambled information put away in cloud by re-appropriating the substantial calculation to cloud specialist co-op (CSP) [4]. Be that as it may, as the measure of encoded documents put away in cloud is winding up extremely gigantic, which will obstruct productive question handling. client can prompt effective encryption/decoding of the information.

EXISTING SYSTEM

This new paradigm of data hosting and data access services introduces a great challenge to data access control. Because the cloud server cannot be fully trusted by data owners, they can no longer rely on servers to do access control. Cipher text-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. In CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution.

Drawback:

Huge issue in Enforcement of authorization policies and the support of policy updates

In 2011, S. Jahid, P. Mittal, and N. Borisov, worked on **"Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation".** The proposed Easier architecture that supports two approaches are fine-grained access control policies and dynamic group membership. Both scheme achieved by using attribute-based encryption, however, is that it is possible to remove access from a user without issuing new keys to other users or re-encrypting existing cipher texts. We achieve this by creating a proxy that participates in the decryption process and enforces revocation constraints. The advantage of this scheme is the Easier architecture and construction provides performance evaluation, and prototype application of our approach on Face book.

PROPOSED SYSTEM

In this paper, we first propose a revocable multi-authority CP-ABE scheme, where an efficient and secure revocation method is proposed to solve the attribute revocation problem in the system. Our attribute revocation 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 (The revoked user cannot decrypt any new cipher text that requires the revoked attribute to decrypt)and forward security (The newly joined user can also

decrypt the previously published ciphertexts1, if it has sufficient attributes). Our scheme does not require the server to be fully trusted, because the key update is enforced by each attribute authority not the server. Even if the server is not semi trusted in some scenarios, our scheme can still guarantee the backward security. Then, we apply our proposed revocable multi-authority CP-ABE scheme as the underlying techniques to construct the expressive and secure data access control scheme for multi-authority cloud storage systems.

III RELATED WORK

In the paper [1] creators explored the two primary instances of access qualification abuse: one is on the semi-trusted expert side, and the other is in favor of cloud client. To moderate the abuse, authors proposed the primary responsible specialist and revocable CP-ABE based distributed storage framework with white-box traceability and reviewing, alluded to as CryptCloud+.

In the paper [2], authors outlined a proficient revocable attribute based encryption (RABE) plot with the property of ciphertext designation.propose a protected and effective fine-grained get to control and information sharing plan for dynamic client bunches by (1) characterizing and upholding access approaches in view of the characteristics of the information; (2) allowing key generation center (KGC) to effectively refresh client certifications for dynamic client gatherings; and (3) permitting some costly calculation errands to be performed by untrusted CSPs without requiring any delegation key.

In the paper[3],creator proposed the Secure Information Sharing in Clouds (SeDaSC) methodology that givesinformation privacy and honesty, get to controlinformation sharing (sending) without utilizing figure concentrated re-encryption, insider risk securityandforward and in reverse access control.

This paper [4] built up another cryptosystem for fine-grained sharing of scrambled information. In this cryptosystem, ciphertexts are named with sets of characteristics and private keys are related with get to structures that control which ciphertexts a client is capable to decode.

This paper [5], proposed a multi-expert ciphertext-approach ABE conspire with responsibility, which permits following the personality of a getting into mischief client who released the decoding key to others, and in this manner diminishes the confide in presumptions on the specialists as well as the clients.

This paper [6], proposes an idea called auditable σ-time outsourced CP-ABE, which is accepted to be appropriate to distributed computing. In this a costly blending activity caused by decoding is offloaded to cloud and in the interim, the rightness of the task can be inspected effectively.

This paper [7], provided an expressive, productive and revocable information get to control plot for multi-expert distributed storage frameworks, where there are various authorities exist together and every specialist can issue properties autonomously. In particular, they proposed a revocable multi-expert CP-ABE conspire, and applied it as the fundamental systems to outline the data access to control plot.

IV. SYSTEM ARCHITECTURE

A revocable multi-authority CP-ABE scheme, to solve the attribute revocation problem in the system. This method is an efficient and secure revocation method. The attribute revocation method can efficiently achieve both forward security and backward security. In backward security scheme the

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 08
July 2019

revoked user cannot decrypt any new Cipher text that requires the revoked attribute to decrypt. In Forward security the newly joined user can also decrypt the previously published cipher texts, if it has sufficient attributes. Moreover, while updating the cipher texts, all the users need to hold only the latest secret key, rather than to keep records on all the previous secret keys.

We consider a data access control system in multi-authority cloud storage, as described in Figure1. There are five types of entities in the system: a certificate authority (CA), attribute authorities (AAs), data owners (owners), the cloud server (server) and data consumers (users).

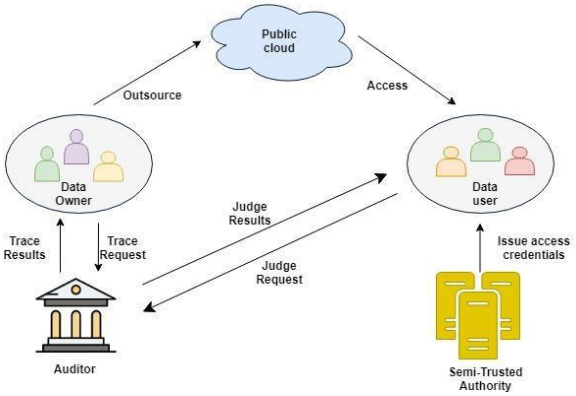

Fig 1: CP-ABE based Cloud storage

Semi-Trusted Authority is semi-trusted as in it might (re-)convey access credentials to the individuals who are unapproved however creates framework parameters (to be imparted to Auditor) sincerely. A completely trusted Auditor keeps a duplicate of the framework parameters shared by Semi-Trusted Authority. Data Owners encode their information to avert unapproved get to. Approved DUs may deliberately release their entrance certifications,for example, pitching accreditations to an outsider. Practically speaking, get to accreditations are probably going to pull in potential purchasers (in dark showcase), and the framework deceivers (offering the certifications) may never have been gotten.

Even though auditors claim to be fully trusted they are never the case. At least one in three shall be a dishonest auditor who wishfully provide incorrect audit results to the data owners. In order to mitigate this, we propose a multiple auditor scheme whose independent audits are compared and the correct audit results are sent to the authorized data owners. Request of tracing from data owners is received by all the auditors and auditing is performed from every independent auditor. These audit results are compared for maximum accuracy in results. Suppose one found to be an improper audit result, then such an auditor is revoked from the system. And the audit result with proper audit is sent back to the data owner.

V. EXPERIMENTAL RESULTS

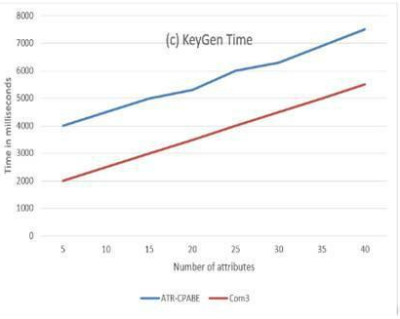

Fig.4.1 Experimental Results

In CP-ABE frameworks, the multifaceted nature of ciphertext arrangement impacts both the encryption time and the unscrambling time. To represent this, we produce ciphertext approaches in the type of (S1 and S2 ... what's more, Sl) to re-enact the most pessimistic scenario circumstance, where Si is a trait. We endeavor to assess the effectiveness of ATR-CP-ABE looking at the aggregate time taken amid each phase with the unique CP-ABE conspire which

does not consider the entrance accreditations mishandle issue and the disavowal issue. As delineated in Fig. 4.1, we look at the time cost of executing singular stage (counting the Encrypt Time, the Decrypt Time and the KeyGen Time (of AT)). Since we consider both access qualification mishandle issue and the denial issue, it isn't shocking to watch that our frameworks require additional time.

- Information owners (IOs) encode their information under the significant access policies preceding redistributing the information to an open cloud/ Public Cloud (PC).
- PC stores the re-appropriated (scrambled) information from IOs furthermore, handles information get to demand from information clients (ICs). PC registers the authorised owners and users.
- Authorized ICs can get to (for example download what's more, decode) the re-appropriated information. PC allows only authorised clients to access the data in cloud.
- Semi-confided in power like Semi-trusted authority (AT) produces framework parameters what's more, issues get to accreditations (i.e., unscrambling keys) to ICs.
- Auditor (AU) is trusted by different substances, takes charge of review and renounce systems, and returns the trace and review results to DOs and DUs.

To deal with the security issue, instead of using the system unique public key (generated by the unique master key) to encrypt data, our scheme requires all attribute authorities to generate their own public keys and uses them to encrypt data together with the global public parameters. This prevent the certificate authority in our scheme from decrypting the cipher texts.

To solve the attribute revocation problem, we assign a version number for each attribute. When an attribute revocation happens, only those components associated with the revoked attribute in secret keys and cipher texts need to be updated. When an attribute of a user is revoked from its corresponding AA, the AA generates a new version key for this revoked attribute and generates an update key. With the update key, all the users, except the revoked user, who hold the revoked attributes can update its secret key (Backward Security). By using the update key, the components associated with the revoked attribute in the cipher text can also be updated to the current version. To improve the efficiency, we delegate the work load of cipher text update to the server by using the proxy reencryption method, such that the newly joined user is also able to decrypt the previously published data, which are encrypted with the previous public keys, if they have sufficient attributes (Forward Security). Moreover, by updating the cipher texts, all the users need to hold only the latest secret key, rather than to keep records on all the previous secret keys.

At a similar time, it can likewise guarantee that semi-believed specialist won't (re-)circulate the made access qualifications to other people, which gave a responsible expert and revocable CP-ABE based distributed storage framework. In any case, one attempting issue in dealing with customer denial in distributed storage is that a repudiated customer may regardless will at

present have the ability to unscramble an old ciphertext they were endorsed to access before being renounced. To address this issue, the ciphertext set away in the distributed storage should be refreshed, ideally by the (untrusted) cloud server. Additionally, it needed planned information getting to control which would give a significant dimension of security.

Looking to relieve access credential abuse, the proposed system uses an authority and revocable CPABE based cloud framework with white-box discernibility and examining. To the best of our insight, this is the primary down to earth answer for secure fine-grained access authority over scrambled information in cloud. In particular, the project presents a CP-ABE based distributed storage structure. Utilizing this (conventional) structure, the proposed system provides two modules, authority and revocable CP-ABE frameworks (with Whitebox discernibility and examining) that are completely secure in the standard model, alluded to as ATER-CP-ABE and ATIR-CPABE, separately. In view of the two frameworks, project gives the following highlights:

Traceability of vindictive cloud clients. Clients who release their entrance qualifications can be followed and distinguished. Accountable authority: A semi-confided in power, who (without appropriate approval) produces and further conveys access qualifications to unapproved user(s), can be distinguished. This enables further activities to be embraced (for example criminal examination or common suit for harms and break of agreement). Auditing: An evaluator can decide whether a (suspected) cloud client is liable in releasing his/her entrance qualification.

V1.CONCLUSION

In this work, we have tried to solve the problem of credential leakage in CP-ABE based distributed storage framework by planning a accountable authority and revocable Cloud++. This is the CP-ABE based distributed storage framework that supports accountable authority, various inspecting and powerful revocation. Specifically, Cloud++ enables us to follow and disavow noxious cloud clients. Our approach can be likewise utilized as a part of the situation where the clients' certifications are redistributed by the semi-put stock in specialist. This likewise gives a timed data access control where client can get to the information inside a determined time for the given key in this manner preventing access to documents by the renounced user. Furthermore, AU is thought to be completely confided in CryptCloud+. Be that as it may, practically speaking, it may not be the situation. so we gave an approach to decrease trust from AU by utilizing various AU's.

REFERENCES

[1] "CryptCloud+: Secure and Expressive Data Access Control for Cloud Storage" Jianting Ning, Zhenfu Cao, Senior Member, IEEE, Xiaolei Dong, Kaitai Liang, Member, IEEE, Lifei Wei, and Kim-Kwang Raymond Choo, Senior Member, IEEE

[2] "Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups

in Cloud" Shengmin Xu, Guomin Yang , Senior Member, IEEE, Yi Mu, Senior Member, IEEE,and Robert H. Deng Fellow, IEEE

[3] Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, and Albert Y. Zomaya. "Sedasc: Secure data sharing in clouds." IEEE Systems Journal, 11(2):395–404,2017.

[4] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. "Attribute-based encryption for fine-grained access control of encrypted data." In Proceedings of the 13th ACM conference on Computerand communications security, pages 89–98. ACM, 2006.

[5] Jin Li, Qiong Huang, Xiaofeng Chen, Sherman SM Chow, Duncan S Wong, and Dongqing Xie. "Multi-authority ciphertext-policy attribute-based encryption with accountability." In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2011, pages 386–390. ACM, 2011.

[6] Jianting Ning, Zhenfu Cao, Xiaolei Dong, Kaitai Liang, Hui Ma, and LifeiWei. 'Auditable -time outsourced attribute-based encryption for access control in cloud computing." IEEE Transactions on Information Forensics and Security, 13(1):94–105, 2018.

[7] Kan Yang, Student Member, IEEE, and Xiaohua Jia, Fellow, IEEE. "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage."

[8] Amit Sahai and Brent Waters. "Fuzzy identity-based encryption." In Advances in Cryptology–EUROCRYPT 2005, pages 457–473.Springer, 2005.

[9] Brent Waters. "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization." In Public Key Cryptography–PKC 2011, pages 53–70. Springer, 2011.

[10] Kan Yang, Zhen Liu, Xiaohua Jia, and Xuemin Sherman Shen. "Time-domain attribute-based access control for cloud-based video content sharing: A cryptographic approach." IEEE Transactions on Multimedia, 18(5):940–950, 2016.

[11] Zhen Liu, Zhenfu Cao, and Duncan S Wong. "Blackbox traceable cp-abe: how to catch people leaking their keys by selling decryption devices on ebay." In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, pages 475–486. ACM, 2013.

Author's Profile:

Suresh Kumar Potnuru
Studying M.Tech (2nd year Pursuing)
Computer Science and Engineering.

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 08
July 2019

Raja Jacob Chidipi
Working as Associate Professor
Qualification MCA, MISTE, M.Tech