Journal of Engineering Sciences
Vol 11, Issue 5,May/2020
ISSN NO:0377-9254

Enhanced data privacy protection based on access control in Cloud

[1]Jemal Yimer Damtew [2]Mrs. M Arathi
[1]M.Tech (CNIS), School of Information Technology, Jawaharlal Nehru Technological University Hyderabad, Telangana, India.
[2]Associate Professor, School of Information Technology, Jawaharlal Nehru Technological University Hyderabad, Telangana, India.

Abstract—***with the quick improvement of PC innovation, cloud-based administrations have become an interesting issue. They furnish clients with accommodation, yet additionally bring numerous security issues, for example, information sharing and protection issue. In this paper, we present an entrance control framework with benefit division dependent on security assurance (PS-ACS). In the PS-ACS conspire, we separate clients into private domain and public domain legitimately. In PRD, to accomplish read get to authorization and compose get to consent, we embrace the Key-Aggregate Encryption and the Improved Attribute-based Signature individually. In Public domain, we build another multi-authority ciphertext policy attribute-based encryption plot with productive unscrambling to keep away from the issues of single purpose of disappointment and confounded key circulation, and plan an effective trait repudiation technique for it. The investigation and reenactment result show that our plan is attainable and better than secure clients' protection in cloud-based administrations.***

Keywords: *access control; data sharing; privacy protection; cloud-based services*

1. INTRODUCTION

With the fast advancement of distributed computing, large information and open cloud administrations have been broadly utilized. Clients can store their information in the cloud support and depend on the cloud specialist organization to give information access to different clients. Nonetheless, the cloud specialist co-op can never again be completely trusted. Since it might give information access to some unlawful clients or aggressors revenue driven addition. For clients, it is important to exploit distributed storage administration, and furthermore to guarantee information protection. Accordingly, the investigation of access control plan to ensure clients' protection in cloud condition is of incredible centrality. Since customary access control technique can't adequately take care of the security issues that exist in information sharing, different plans to accomplish encryption and decoding of information sharing have been proposed.

In 2007, Bethencourt et al. first proposed the ciphertext strategy trait based encryption (CP-ABE). Be that as it may, this plan doesn't think about the denial of access consents. Attrapadung et al. concocted two client revocable ABE conspire. In any case, they are not relevant in the re-appropriating condition. In 2011, Hur et al. set forward a finegrained disavowal conspire, however it can without much of a stretch reason key escrow issue. Lewko et al. utilized multi-authority ABE (MA-ABE) to explain key escrow issue. However, the entrance strategy isn't adaptable. Afterward, Li et al. introduced an information sharing plan dependent on foundational quality encryption, which invests diverse access authorizations to various clients. Nonetheless, it absences of effectiveness. Xie et al. introduced a revocable CPABE conspire. Contrasted and Hur's plan, in the key update stage, the calculation heap of the information administration chief will be diminished considerably. Liang et al. proposed a CP-ABE intermediary encryption plot which bolsters any monotonic access structures.

2. RELATED WORK

Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing [1]

Distributed computing is a rising processing worldview in which assets of the figuring framework are given as administrations over the Internet. As promising as it seems to be, this worldview likewise delivers numerous new difficulties for information security and access control when clients redistribute touchy information for sharing on cloud servers, which are not inside a similar confided in space as information proprietors. To keep delicate client information classified against untrusted servers, existing arrangements as a rule apply cryptographic techniques by revealing information unscrambling keys just to approved clients. Be that as it may, in doing as such, these arrangements unavoidably present a substantial calculation overhead on the information proprietor for key dissemination and information the executives when finegrained information get to control is wanted, and hence don't scale well. The issue of at the same time accomplishing fine-grainedness, adaptability, and information privacy of access control in reality despite everything stays uncertain. This paper tends to this difficult open issue by, on one hand, characterizing and implementing access approaches dependent on information traits, and, then again, permitting the information proprietor to designate the majority of the calculation undertakings associated with finegrained information get to control to untrusted cloud servers without unveiling the hidden information substance. They accomplish this objective by misusing and particularly consolidating strategies of quality based encryption (ABE), intermediary re-encryption, and languid re-encryption. Their proposed plot additionally has striking properties of client get to benefit privacy and client mystery key responsibility. Broad investigation shows that their proposed conspire is exceptionally effective and provably secure under existing security models.

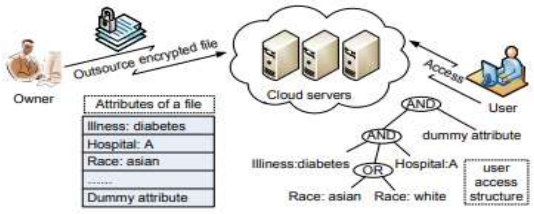

Fig.1: An examplary case in the healthcare scenario

This paper focuses on fine-grained information get to control in distributed computing. One test in this setting is to accomplish finegrainedness, information classification, and adaptability at the same time, which isn't given by current work. In this paper they proposed a plan to accomplish this objective by abusing KPABE and extraordinarily consolidating it with methods of intermediary re-encryption and lethargic re-encryption. Besides, their proposed plan can empower the information proprietor to assign the majority of calculation overhead to ground-breaking cloud servers. Classification of client get to benefit and client mystery key responsibility can be accomplished. Formal security proofs show that our proposed conspire is secure under standard cryptographic models.

Attribute-Based Encryption Supporting Direct/Indirect Revocation Modes [4]

Attribute-based encryption (ABE) empowers an entrance control component over scrambled information by determining access strategies among private keys and ciphertexts. In this paper, they center around ABE that underpins denial. At present, there are two accessible revocable ABE conspires in the writing. Their disavowal systems, in any case, vary as in they can be considered as immediate and aberrant strategies. Direct disavowal authorizes renouncement straightforwardly by the sender who determines the denial list while encoding. Backhanded disavowal upholds denial by the key power who discharges a key update material occasionally so that just non-repudiated clients can refresh their keys (thus, renounced clients' keys are certainly rendered pointless). A preferred position of the roundabout strategy over the immediate one is that it doesn't expect senders to realize the renouncement list. Conversely, a bit of leeway of the

immediate technique over the other is that it doesn't include key update stage for all non-renounced clients communicating with the key position. In this paper, they presented the main Hybrid Revocable ABE conspire that permits senders to choose on-the fly while scrambling whether to utilize either immediate or circuitous repudiation mode; hence, it joins best favorable circumstances from the two strategies.

Creator introduced a formalization and a development of half and half revocable quality based encryption. A HR-ABE framework permits senders to choose whether to utilize either immediate or roundabout denial mode while encoding a message. With direct mode, the sender indicates the rundown of repudiated clients straightforwardly into the encryption calculation. With backhanded mode, the sender determines only the scramble time (other than a typical property set), while beneficiaries acquire a key update material at each schedule opening to refresh their keys from the power, but so that solitary no repudiated clients can refresh (subsequently disavowal is authorized by implication). Their HR-ABE conspire requires every beneficiary to store just one key, which is in any case can be utilized to decode ciphertexts in either mode. The key size in our cross breed plot is generally equivalent to that of the two as of now best one-mode revocable plans. They demonstrated the security for the specific objective and semi-static question model under the DBDH presumption.

3. FRAMEWORK

In this paper, we present a more systematic, flexible and efficient access control scheme. We propose a novel access control system called PS-ACS, which is privilege separation based on privacy protection. To achieve read access permission, in PRD, the Key-Aggregate Encryption (KAE) scheme which greatly improves access efficiency is adopted. And in PUD, we construct a new multi-authority ciphertext policy attribute-based encryption (CP-ABE) scheme with efficient decryption to avoid the issues of single point of failure and complicated key distribution, and design an efficient attribute revocation method for it. Compared with the MAH-ABE scheme which does not refer to the write access control, we exploit an Improved Attribute-based Signature (IABS) scheme to enforce write access control in PRD.

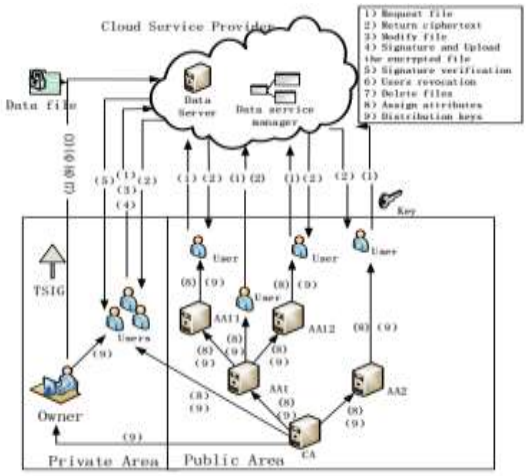

Fig.2: System framework

In this way, the user can pass the cloud server's signature verification without disclosing the identity, and successfully modify the file. We provide security and performance analysis of our proposed PS-ACS scheme. The functionality and simulation results provide data security in acceptable performance impact, and prove the feasibility of the scheme.

Our system model consists of Data owners, users in PRD, and users in PUD, a global certificate authority (CA), attribute authorities (AA) and the cloud service provider, which are defined as follows.

1) The cloud service provider consists of two parts: data storage server and data service management. Data storage server is responsible for storing confidential data fi les, and data service management is in charge of controlling external users' access to secret data and returning the corresponding ciphertext.

2) In the actual cloud environment, CA manages multiple AAs, and each AA manages attributes in their own fi eld. The attributes owned by the user are issued by different authorities.

3) Users in private domain (PRD) have special privileges, such as family, personal assistant, close friends and partners. This domain has a small number

of users and small scale attributes, and the data owner knows users' identities, which is easy to manage.

4) In public domain (PUD), there exist a huge number of users with unknown identities and a lot of attributes owned by the user.

5) Data Owner can develop different access control strategies based on the characteristics of users in public and personal domain, encrypt uploaded files using the corresponding encryption method and then send them to the cloud server.

Algorithm:

Ciphertext Policy Attribute Based Encryption Scheme:

Setup: This algorithm takes as input the security parameter κ, and returns a public key PK and a master secret key MK.

KeyGen: This algorithm takes as input PK, MK and a set of attributes L, and returns a secret key SKL associated with L.

Encrypt: This algorithm takes as input PK, a message M and an access structure W. It returns a ciphertext C with the property that a user with SKL can decrypt C if and only if L |= W.

Decrypt: This algorithm takes as input PK, C which was encrypted by W, and SKL. It returns M if SKL is associated with L |= W.

4. EXPERIMENTAL RESULTS

Our plan bolsters effective client and trait repudiation without refreshing clients' private keys. For client disavowal, we don't have to re-encode the ciphertext and update all non-renounced clients' private keys. Rather, we just need to erase the client's change keys. Without the change key, he can no longer decode the ciphertext. Then again, when characteristic renouncement happens, private keys of all non-denied clients won't be refreshed, just the change keys which are put away in the cloud server and the included ciphertext should be refreshed. In this manner, the productivity of denial can be significantly improved.

We analyzed the figuring time caused in encryption and unscrambling. In Fig.3, the quantity of specialists is set to 10. Clearly our plan requires less time for encryption and unscrambling than Ruj's plan, particularly for decoding. Since in the decoding stage, significant calculation overhead is designated to the cloud, client just needs one exponentiation activity to recoup the first message.

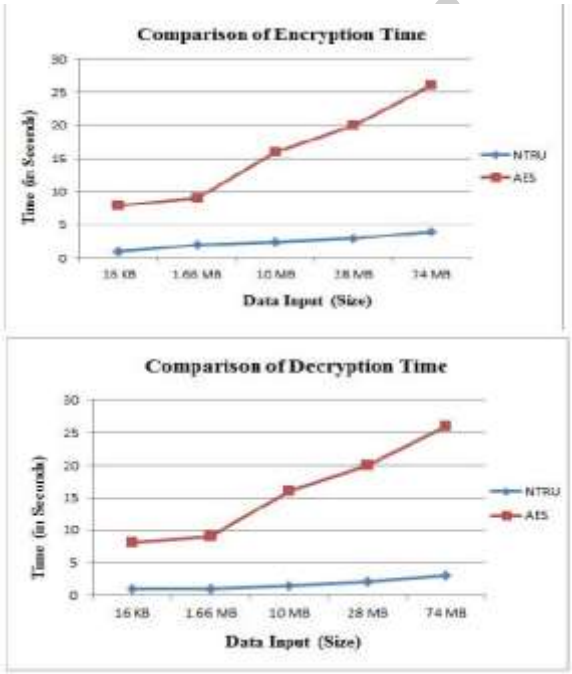

Fig.3: Comparison of Encryption and Decryption Time

Therefore, the decryption time for users can be greatly reduced.

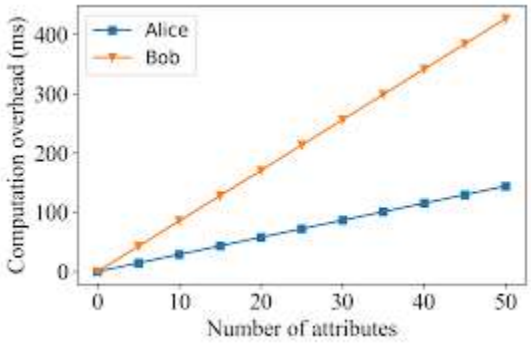

Fig.4: Computing cost for transformation

Computing cost for transformation is shown in Fig.4. On the whole, it can be concluded that our scheme's computation efficiency is much better than Ruj's scheme.

5. CONCLUSION

In this paper, we proposed an access control system (PS-ACS), which is benefit division dependent on security assurance. Through the examination of cloud condition and the qualities of the client, we partition clients into Private domain and public domain intelligently. In PRD, we set peruse and compose get to consents for clients individually. To accomplish read get to authorization, the KAE plot which can improve the entrance efficiency is received. A high level of patient security is ensured at the same time by utilizing IABS plot which can decide clients' compose get to consent. For clients in PUD, we built another multi-authority ciphertext policy attribute-based encryption (CP-ABE) plot with productive unscrambling to stay away from the issues of single purpose of disappointment and confounded key appropriation, and plan an effective quality disavowal technique for it. The examination and the reproduction result show that the PSACS conspire is attainable and better than secure the protection of information in cloud-based administrations.

REFERENCES

[1] YU SH, WANG C, REN K, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing", Proceedings of IEEE Con-ference on Information Communications 2010, pp. 1-9, 2010.

[2] BETHENCOURT J, SAHAI A, WATERS B, "Ciphertext-Policy Attribute-based Encryption", IEEE Symposium on Security and Privacy, vol. 2008, no. 4, pp. 321-334, 2007.

[3] ATTRAPADUNG N, IMAI H, "Conjunctive Broadcast and Attribute-Based Encryption", Proceedings of Pairing-based Cryptography - Pairing 2009, vol. 5671, pp. 248-265, 2009.

[4] ATTRAPADUNG N, IMAI H, "Attribute-Based Encryption Supporting Direct/Indirect Revocation Modes", Proceedings of Cryptography and Coding 2009, pp. 278-300, 2009.

[5] HUR J, NOH D K, "Attribute-based Access Control with Efficient Revocation in Data Outsourcing Systems", IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, 2011.

[6] LEWKO A, WATERS B, "Decentralizing Attribute-based Encryption", Proceedings of Advances in Cryptology-EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 568-588, 2011.

[7] LI M, YU SH, ZHENG Y, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-based Encryption", IEEE Transactions on Parallel and Distributed System, vol. 24, no. 1, pp. 131-143, 2013.

[8] XIE X, MA H, LI J, et al, "New Ciphertext-Policy Attribute-based Access Control with Efficient Revocation", Proceedings of Information and Communication Technology 2013, pp. 373-382, 2013.

[9] LIANG K, MAN H A, SUSILO W, et al, "An Adaptively CCA-Secure Ciphertext-Policy Attribute-Based Proxy Re-Encryption for Cloud Data Sharing", Information Security Practice and Experience, pp. 448-461, 2014.

[10] CHU C K, CHOW S S M, TZENG W G, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 468- 477, 2014.