Implementation of Ciphertext-policy attribute-based encryption (CP-ABE) scheme for Cloud Data Storage

Nalamothu Aravind #1, Perla Nikhila #2, Jedi Venkata Sasank #3, Cheemaladinna Balaji #4, Dhulipalla Vignan #5, K V S Bharath Kumar #6

#1 Assistant professor, Dept Of CSE, QIS College of Engineering and Technology, Ongole, Prakasam (Dt)
#2 Student, Dept Of CSE, QIS College of Engineering and Technology, Ongole, Prakasam (Dt)
#3 Student, Dept Of CSE, QIS College of Engineering and Technology, Ongole, Prakasam (Dt)
#4 Student, Dept Of CSE, QIS College of Engineering and Technology, Ongole, Prakasam (Dt)
#5 Student, Dept Of CSE, QIS College of Engineering and Technology, Ongole, Prakasam (Dt)
#6 Student, Dept Of CSE, QIS College of Engineering and Technology, Ongole, Prakasam (Dt)

Abstract: Ciphertext-strategy trait based encryption (CP-ABE) conspire is another sort of information encryption crude, which is entirely appropriate for information distributed storage for its fine-grained get to control. Watchword based accessible encryption plot empowers clients to rapidly discover fascinating information put away in the cloud server without uncovering any data of the looked through catchphrases. In this work, we give a catchphrase accessible property based encryption conspire with characteristic update for distributed storage, which is a blend of trait based encryption plan and watchword accessible encryption plot. The new plan bolsters the client's quality update, particularly in our new plan when a client's credit should be refreshed, just the client's mystery key related with the ascribe should be refreshed, while other client's mystery key and the figure messages related with this credit need not to be refreshed with the assistance of the cloud server. Furthermore, we redistribute the activity with high calculation cost to cloud server to decrease the client's computational weight. Also, our plan is demonstrated to be semantic protection from picked ciphertext-strategy and picked plaintext assault in the general bilinear gathering model. What's more, our plan is additionally demonstrated to be semantic protection from picked catchphrase assault under bilinear Diffie-Hellman (BDH) presumption

Keywords: Attribute-based encryption, Access control, Keyword search.

I. INTRODUCTION

Characteristic based encryption (ABE) [1–4] is viewed as a powerful encryption technique with fine grained get to control in the distributed storage. Quality based encryption can be separated into two sorts of key-arrangement characteristic based encryption [1] (KP-ABE) and ciphertext-strategy trait based encryption [2] (CP-ABE). The KP-ABE conspire alludes to that the ciphertext is related with a trait set, and a client's mystery key is related with an entrance strategy. A client can unscramble the ciphertext if and just if the ciphertext's quality set fulfill the entrance strategy of client's mystery key. The CP-ABE plot alludes to that the ciphertext is related with an entrance strategy, and a client's mystery key is related with a property set. A client is can unscramble the ciphertext

if and just if his property set fulfill the entrance strategy of the ciphertext.

At present, numerous ABE plans [5–9] have been proposed, which give secure information get to control and beat the inadequacies of balanced encryption design in personality based encryption plot. Be that as it may, these plans are as yet imperfect to be utilized by and by, as the trait of a client is dynamic, which might be changed after some time. Therefore the trait repudiation instrument is fundamental for ABE plan to be utilized by and by.

The repudiation instrument can be separated into two sorts: direct denial system and circuitous disavowal component. Imai and Attrapaduang [10] give an away from of direct disavowal and backhanded renouncement. Direct disavowal is characterized as: the sender indicates a repudiation list while encoding the information. Backhanded repudiation is characterized as: the approved establishments normally issue key updates to non-disavowed clients. At present, numerous plans with direct disavowal [11–14] have been proposed. Li et al. [11] proposed a character based renouncement plot that performs coordinated denial by giving the disavowal rights to encipherer legitimately. Tu et al. [14] proposed a revocable ABE conspire. Furthermore, some roundabout quality repudiation schemes[15–18] have additionally been proposed. Yu et al.[15] proposed a trait based information imparting plan to characteristic disavowal. In this plan, client's any property can be denied as a substitute re-encryption strategy. Li et al. [18] proposed a plan that underpins client's quality denial, yet the plan could just repudiate a solitary characteristic of the client, in this manner it couldn't fulfill the genuine needs.

The property update is another huge issue in the ABE condition. In real life, a client's credit set may should be refreshed after some time when his working job might be changed. For instance, accept that Alice is an organization worker, at that point her ascribe set should be refreshed when her working job is advanced from a software engineer lifted to a venture chief, in this manner her previous quality set A = "female, developer" ought to be changed to another property set B = "female, venture supervisor". Also, the characteristic position (AA) should give an update key to refresh

Alice's mystery key. In the interim, the characteristic position must guarantee that the representative Alice can't further utilize her past key identified with the trait set "female, developer" to get to the figure messages. Subsequently, the trait update is certainly not a straightforward procedure. Some quality update plans [19–21] have been proposed. Notwithstanding, these plans have a typical issue, the issue is that on the off chance that there is a client's a trait is refreshed, and afterward numerous other client's mystery key and a great deal of figure messages related with this credit should be refreshed, which will without a doubt squander a ton of computational assets.

To address this issue, we give a plausible arrangement in this paper. The principle thought of our answer is that the mystery key of a client is partitioned into two sections, one section which is insignificant to characteristic is held by the client, and the other part which is applicable to ascribe is sent to the cloud server (CS). At the point

when a quality of any client should be refreshed, the AA gives an update key to CS. At that point CS just updates the mystery key of this characteristic for every legitimate client, and other mystery key of all client and the figure messages related with this credit need not to be refreshed. This technique will enormously lessen the outstanding task at hand of the framework.

Although attribute based encryption technology provides an effective means for data confidentiality, yet it brings another new problem that the users may find it difficult to search for interesting data from a vast number of encrypted data. This problem is called keyword search problem [22]. One of the simplest searching methods is to download all encrypted data locally and then to decrypt it, finally to execute keyword search in plaintext. However, this method will waste huge computational resource and bring a vast cost for user to do the work of decryption.

Another extreme searching method is to send the secret key of the user and keywords to CS, then CS decrypts all of the cipher texts and performs searching operation on plaintext. But this method will expose the user's secret key and privacy of search keyword to CS, this is infeasible. Some search-based encryption schemes [13–16] have been proposed. Such as Boneh et al. [3] first proposed a public key encryption with keyword search scheme. Dan and Ostrovsky [14] proposed a public key cryptographic scheme that allows privacy data retrieval (PIR), and allows multiple data contributors to upload their data with public key by encryption algorithm, and only the user with the corresponding secret key can decrypt the data.

II RELATED WORK

The endeavors of researcher and analyst in cryptography accomplish their own strategies in various field of cryptography for the reasons for information security. In any case, after the advancement of character based encryption in cryptography that dependent on fluffy personality encryption in [1] thought of characteristic based encryption the quality set speaks to characters the information sender need to determine a few traits for the information beneficiary no need of indicate with explicit personality where the trait based encryption has pleasant property that give information get to control the unscrambling side are not fixed. At that point Ostrovsky et al in [10] proposed quality based encryption plan of private keys for any entrance structure of Boolean equation that handle AND\OR entryway including non-monotonic access structure one. After that Goyal et al [2] and Bethencourt [3] proposed for (KP-ABE) and (CP-ABE) put together that based with respect to property base encryption for the information get to control get to strategy for security and protection. Consistent size ciphertext is additionally a sort of ABE in examine bearing.

Doshi et al [11] proposed completely secure steady size (CP-ABE) plan to learn about the entrance structure of credits with mystery key to an any subset of characteristic can be a piece of ciphertext strategy which makes the security issues for the proposed plot. There are numerous multi authority property based encryption Yang et al [12,13,14] has been proposed for secure information get to control that accomplish the characteristic disavowal under arbitrary prophet model yet these plan can't approach

about the effective access strategy changes to new arrangement in quality denial for the scrambled information that give forward security. Chen et al [15] introduced a safe trait based encryption conspire with edge get to structure for consistent ciphertext in property based encryption and characteristic based mark ABE/ABS. Further his plan plot bolster both KP-ABE and (CP-ABE) that material to enormous characteristic universe with consistent size ciphertext with ABS and lessen a blending assessment to a steady size, that has a decent property for down to earth quality based encryption however his plan can't bolster catchphrase search and denial. Qiu et al [16] formulized covered up ciphertext strategy trait based encryption catchphrases search conspire in which any client's just ready to access and search the watchwords if he\she fulfill the entrance strategy of the information proprietor encoded information and demonstrate that his plan makes sure about under general gathering model for undefined against watchwords with get to structure. Ciu et al [17] put a forward CP-ABE Scheme with mostly shrouded get to strategy with get to structure give trait's name, property's estimations are not given in the ciphertext where his plan can't bolster the characteristic repudiation and information certainty that remaining parts. After that Wang et al [18] introduced a catchphrase accessible quality based encryption and renouncement conspire if the trait set fulfill the entrance strategy given token match to the watchword list the particular client's will have the option to get the join catchphrases inquiry, however his plan can't clear about AND/OR entryway get to strategy hence the plan can't accomplish both AND/OR door get to strategy just help AND entryway get to strategy. To take care of this issue, the Yin et al [19] proposed a proficient Ciphertext strategy quality based accessible encryption plan and support AND/OR doors get to strategy with edge entryways yet his plan the inquiry token deterministic the question watchwords in trapdoor powerless against picked plain content assault. Lai et al [20] proposed irrefutable ABE re-appropriate unscrambling some additional data are included ciphertext for the confirmation and change result rightness check evidence likewise his plan support re-appropriate decoding.

Zhang et al [21] introduced adaptively secure multi authority ABE that help re-appropriates decoding check however his plan can't bolster re-appropriate encryption and obviousness. Wang et al [22] proposed Verifiable and multi watchwords accessible characteristic based encryption conspire for multi catchphrases the CS doesn't take in any data from catchphrases search trapdoor however his structure plot can't bolster property denial. Xiong et al [13] proposed a complicated Encryption Service Provider (ESP) verifiable scheme for outsource decryption result can be checked by the user’s. Where they demonstrate that the intermediate ciphertext return to the user’s by using either ESP scheme without any detection. In this paper we propose verifiable ciphertext policy attribute based encryption scheme keywords search and attribute revocation. Our VCP-ABE scheme consists secret key generation verification, outsource encryption, outsource decryption, and ciphertext update verification to ensure that

ciphertext successfully update only non-revoked attribute users can access to new encrypted and updated data.

III METHODOLOGY

In this paper, we propose a watchword accessible characteristic based encryption plot with trait update for distributed storage. The primary commitments of our plan are summed up as follows:

The new plan is a blend of ABE plan and watchword accessible encryption conspire. So our plan not just tackles the issue of secrecy of the information with fine grained get to control yet additionally takes care of the issue of catchphrase search. Additionally, the plan is demonstrated to be semantic protection from picked ciphertext-strategy and picked plaintext assault in the general bilinear gathering model.

The new plan underpins the client's trait update, and when a client's ascribe should be refreshed, just the client's mystery key related with this credit should be refreshed, while other clients' mystery key and the figure messages related with the ascribe need not to be refreshed. This is a more effective quality update strategy than that in existing property update plans.

IV SYSTEM MODEL

A system framework of our scheme includes the main four entities is presented in Fig.

Attribute authority (AA): The AA is a perfectly trusted entity. It takes charge of the system establishment, user registration, attributes management and secret key generation. And when an attribute of a user needs to be updated, the AA generates an updated key for the user.

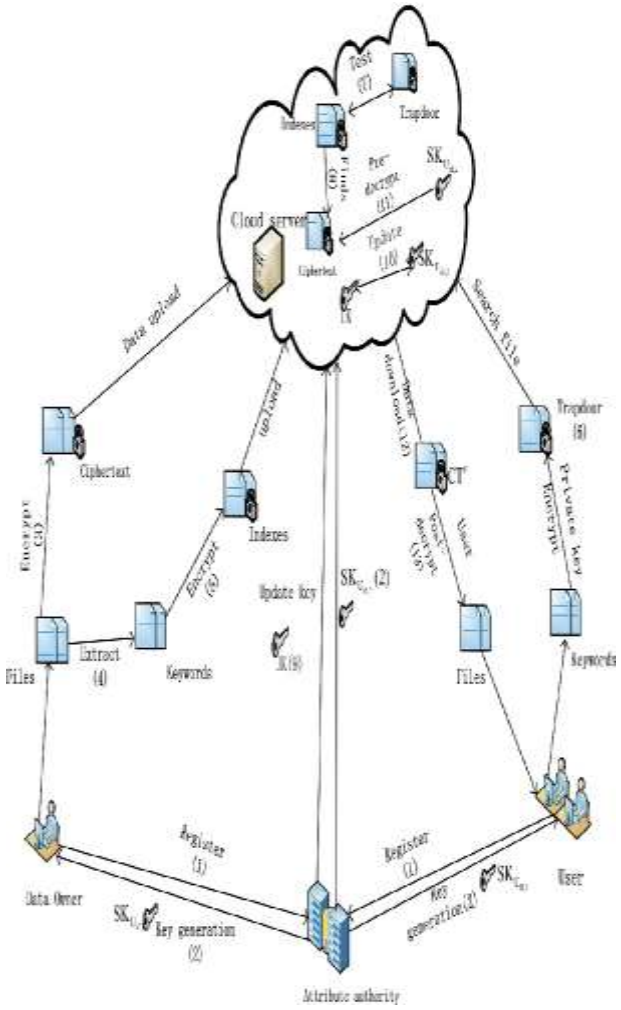

Fig 1: System Model

Cloud server (CS): The CS is liable for putting away the information and giving information access to genuine clients. It is likewise liable for watchword search when an inquiry trapdoor is gotten from a client. What's more, it additionally assumes responsibility for refreshing the client's fractional mystery key which identified with the refreshed trait and legitimates clients to

mostly unscramble the ciphertext by utilizing incomplete mystery key of the client.

Information proprietor (DO): The information proprietor encodes its proprietor information and fabricates catchphrase records, and afterward re-appropriates them to the CS.

Client (U): Each genuine client can look through their fascinating the documents from framework. The client creates an inquiry trapdoor to ensure the security of the pursuit catchphrase. At that point the client sends his personality and search trapdoor to CS. Without uncovering any data about watchword search, the CS will discover the encoded document incorporates the catchphrases and do a ton of halfway decoding work to lessen the unscrambling heap of the client. At long last, the client gets the halfway decoded records, and afterward unscrambles the incomplete unscrambled documents by utilizing his proprietor fractional mystery key.

V CONCLUSION

In this paper, we have proposed an outline of catchphrase accessible trait based encryption plot with quality update for distributed storage. Our new plan underpins both the client's quality update and supports multi-client watchwords search, as long as client's trapdoor could coordinate catchphrase record put away in the distributed storage, at that point the client can look through intriguing scrambled document effectively. For additional the exhibition assessment results might be examined to affirm that the proposed conspire is more proficient than other property based encryption plans with trait update. Also, we re-appropriate the activity with high calculation cost to the distributed storage to lessen the client's computational weight. Besides, our plan likewise is demonstrated to be semantic protection from picked ciphertext-strategy and picked plaintext assault in the general bilinear gathering model.

VI REFERENCES

[1] Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data[C]// ACM Conference on Computer and Communications Security. ACM, 2006:89–98.

[2] Bethencourt J,Sahai A, Waters B. Ciphertext-Policy Attribute-Based Encryption[C]// IEEE Symposium on Security and Privacy. IEEE Computer Society, 2007:321–334.

[3] Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with non-monotonic access structures[C]// Ccs 07 Acm Conference on Computer & Communications Security. 2007:195–203.

[4] Waters B. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization[J]. Lecture Notes in Computer Science, 2011, 2008:321–334.

[5] Chase M, Chow S S M. Improving privacy and security in multi-authority attribute-based encryption[C]// ACM Conferenceon Computerand

Communications Security. ACM, 2009:121–130.

[6] Hur J. Improving Security and Efficiency in Attribute-Based Data Sharing[J]. Knowledge & Data Engi- neering IEEE Transactions on, 2013, 25(10):2271–2282.

[7] Liu X, Ma J, Xiong J, Li Q, Ma J. Ciphertext-Policy Weighted Attribute Based Encryption for Fine- Grained Access Control[C]// International Conference on Intelligent NETWORKING and Collaborative Systems. IEEE, 2014:51–57.

[8] Lai J, Deng R H, Li Y, Weng J. Fully secure key-policy attribute-based encryption with constant-size ciphertexts and fast decryption[C]// ACM Symposium on Information, Computer and Communications Security. ACM, 2014:239–248.

[9] Horva´th M. Attribute-Based Encryption Optimized for Cloud Computing[M]// SOFSEM 2015: Theory and Practice of Computer Science. Springer Berlin Heidelberg, 2015:1–9.

[10] Attrapadung N, Imai H. Attribute-Based Encryption Supporting Direct/Indirect Revocation Modes[C]// Ima International Conference on Cryptography and Coding. Springer-Verlag, 2009:278–300.

[11] Li Y, Zhu J, Wang X, Shao S. Optimized Ciphertext-Policy Attribute-Based Encryption with Efficient Revocation[J]. International Journal of Security & Its Applications, 2013, 7(6):385–394.,

[12] Zhang Y, Chen X, Li J, Li H, Li F. FDR-ABE: Attribute-Based Encryption with Flexible and Direct Revo- cation[C]// International Conference on Intelligent NETWORKING and Collaborative Systems. IEEE, 2013:38–45.

[13] Wang H, Zheng Z, Wu L, Li P. New directly revocable attribute-based encryption scheme and its appli- cation in cloud storage environment [J]. Cluster Computing, 2016:1–8.

[14] Tu S, Niu S, Li H. A fine-grained access control and revocation scheme on clouds[J]. Concurrency & Computation Practice & Experience, 2016, 28(6):1697–1714.

[15] Yu S, Wang C, Ren K, Lou W. Attribute based data sharing with attribute ACM revocation [C]//Sympo- siumon Information, Computer and Communications Security, ASIACCS 2010, Beijing, China, April. DBLP, 2010:261–270.

[16] Qian H, Li J, Zhang Y, Han J. Privacy-preserving personal health record using multi-authority attribute- based encryption with revocation [J]. International Journal of Information Security, 2015, 14(6):487– 497.

[17] Huang X F, Tao Q, Qin B D, Liu Z Q. Multi-Authority Attribute Based Encryption Scheme with Revoca- tion[C]// International Conference on Computer Communication and Networks. IEEE, 2015:1–5.

[18] Li Q, Feng D, Zhang L. An attribute based encryption scheme with fine-grained attribute revocation[C]// Global Communications Conference. IEEE, 2012:885-89-890.

[19] Zhang P, Chen Z, Liang K, Wang S, Wang T. A Cloud-Based Access Control Scheme with User Revo- cation and Attribute

Update[C]// Asian Conference on. Springer-Verlag New York, Inc. 2016:525–540.

[20] Liao J, Jiang C, Guo C. Data privacy protection based on sensitive attributes dynamic update[C]// Inter- national Conference on Cloud Computing and Intelligence Systems. IEEE, 2016:377–381.

[21] Zhang P, Chen Z, Liu J K, Liang K, Liu H. An efficient access control scheme with outsourcing capability and attribute update for fog computing [J]. Future Generation Computer Systems, 2016.

[22] Song D X, Wagner D, Perrig A. Practical Techniques for Searches on Encrypted Data[C]// Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2002:44.

[23] Dan B, Crescenzo G D, Ostrovsky R, Persiano G. Public Key Encryption with Keyword Search[J]. Lec- ture Notes in Computer Science, 2003, 3027(16):506–522.

Authors Profile

Nalamothu Aravind, M.Tech., is working as an Assistant Professor in the department of Computer Science & Engineering in QIS College of Engineering and Technology (Autonomous), Ongole, Andhra Pradesh, India.

Perla Nikhila pursuing B.Tech., in the department of Computer Science & Engineering in QIS College of Engineering and Technology (Autonomous), Ongole, Andhra Pradesh, India.

Jedi Venkata Sasank pursuing B.Tech., in the department of Computer Science & Engineering in QIS College of Engineering and Technology (Autonomous), Ongole, Andhra Pradesh, India.

Cheemaladinna Balaji pursuing B.Tech., in the department of Computer Science & Engineering in QIS College of Engineering and Technology (Autonomous), Ongole, Andhra Pradesh, India.

Dhulipalla Vignan pursuing B.Tech., in the department of Computer Science & Engineering in QIS College of Engineering and Technology (Autonomous), Ongole, Andhra Pradesh, India.

K V S Bharath Kumar pursuing B.Tech., in the department of Computer Science & Engineering in QIS College of Engineering and Technology (Autonomous), Ongole, Andhra Pradesh, India.