

**REDUCE THE DIVISION COST OF OUTSOURCE AND HIGH  
COMPUTATION LOAD TO CLOUD SERVICE PROVIDERS WITHOUT  
DISCLOSE FILE CONTENT AND SECRET KEYS**

<sup>1</sup>Sunil Kumar, <sup>2</sup>Devraj, <sup>3</sup>M.Arvindhan

<sup>1</sup>Assistant Professor, School of Computer Science and Engineering, Galgotias University, GR. Noida, UP, India

<sup>2</sup>Assistant Professor, School of Computer Science and Engineering, Galgotias University, GR. Noida, UP, India

<sup>3</sup>Assistant Professor, School of Computer Science and Engineering, Galgotias University, GR. Noida, UP, India

**ABSTRACT:** *To explain this attack, a concrete instance is offered. We prove the safety in our plan underneath the divisible computation Diffie-Hellman (DCDH) assumption. Regrettably, ABE plan requires high computation overhead during performing file encryption and understanding operations. Within the existing plan, whenever a user leaves from the user group, the audience manager only revokes his group secret key which means the user's private key connected with attributes continues to be valid. Our plan is appropriate for resource restricted devices. If a person within the group intentionally exposes the audience secret answer to the revoked user, he is able to perform understanding operations through his private key. This defect gets to be more severe for lightweight devices because of their restricted computing sources. Within this system, we concentrate on designing a Club penguin-ABE plan with efficient user revocation for cloud storage system. Caused by our experiment shows computation cost for local devices is comparatively low and could be constant. We try to model collusion attack done by revoked users cooperating with existing users. In addition, we construct a competent user revocation Club penguin-ABE plan through increasing the existing plan and prove our plan is CPA secure underneath the selective model.*

**Keywords:** *outsourced encryption, cloud computing, collusion attack, attribute-based encryption, user revocation.*

### 1. INTRODUCTION:

To lessen the computation cost, we delegate high computation load to cloud providers without dripping file content and secret keys. Particularly, our plan can with stand collusion attack done by revoked users cooperating with existing users. To lessen the computation cost for resource-restricted devices, some cryptographic operations rich in computational load were outsourced to cloud providers [1]. The problem of user revocation could be solved efficiently by presenting the idea of user group. When any user leaves, the audience manager will update users' private keys aside from individuals who've been revoked. Furthermore, Club penguin-ABE plan has heavy computation cost, because it grows linearly using the complexity for that access structure. Combined proxy re-file encryption with lazy re-file encryption technique, Eco-friendly et al. provided a competent Club penguin-ABE plan with outsourcing understanding. Within their plan, user's private secret is blinded through utilizing a random number. Both private key and also the random number are stored secret through the user. The consumer shares his blinded private answer to a proxy to do outsourced understanding operation [2]. To be able to safeguard privacy from the user, Han et al. presented a decentralized KP-ABE plan with privacy-preserving. Similarly, Qian et al. provided a decentralized Club penguin-ABE with fully hidden access structure. In the following paragraphs, we concentrate on designing a Club penguin-ABE plan with efficient user revocation for cloud storage system. We try to model collusion attack done by revoked users cooperating with existing users. Can't. When user<sub>1</sub> is revoked in the group, he can't decrypt alone because he doesn't possess the updated group secret key. We construct a competent user revocation Club penguin-ABE plan through increasing the plan and prove our plan is CPA secure underneath the selective model. To resolve above security issue, we embed certificates into each user's private key. The consumer shares his blinded private answer to a proxy to do outsourced understanding operation. Within this paper, we make use of the similar techniques regarding ex-tend our plan with outsourcing ability.

## 2. TRADITIONAL MODEL:

Boldyreva et al. presented an IBE plan with efficient revocation, also is appropriate for KP-ABE. Nonetheless, it's not obvious whether their plan is appropriate for Club penguin-ABE. Yu et al. provided a characteristic based data discussing plan with attribute revocation ability. This plan was demonstrated to become secure against selected plaintext attacks (CPA) according to DBDH assumption. However, the size of cipher text and user's private key are proportional to the amount of attributes within the attribute world. Yu et al. developed a KP-ABE plan with fine-grained data access control. This plan mandates that the main node within the access tree is definitely an AND gate and something child is really a leaf node that is connected using the dummy attribute [3]. Think that the information is encrypted underneath the policy "professor AND cryptography" and also the group public key. Suppose there are two users: user1 and user2 whose private keys are connected using the attribute sets and correspondingly. If are both within the group and contain the group secret key, then user1 can decrypt the information but user2 can't. When user1 is revoked in the group, he can't decrypt alone because he doesn't possess the updated group secret key. However, the features of user1 are not revoked and user2 has got the updated group secret key. So, user1 can collude with user2 to do the understanding operation. In addition, security model and proof weren't provided within their plan. Disadvantages of existing system: It's costly in communication and computation cost for users [4]. There's a significant limitation to single-authority ABE as with IBE. Namely, each user authenticates him towards the authority, proves he includes a certain attribute set, after which receives secret key connected with every of individuals attributes. Thus, the authority should be reliable to watch all of the attributes. It's not reasonable used and cumbersome for authority [4].

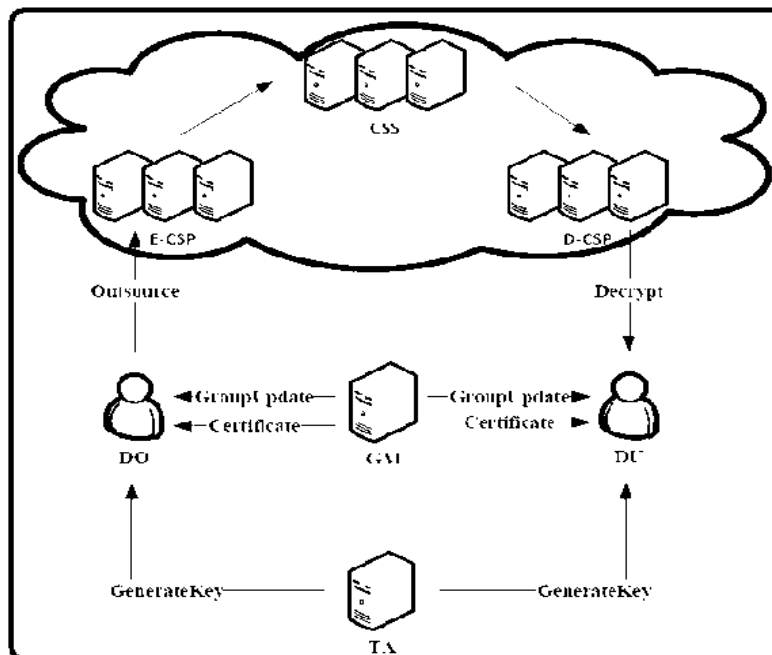


Fig.1. System Framework

## 3. COLLUSION FREE SCHEME:

Within this system, we concentrate on designing a Club penguin-ABE plan with efficient user revocation for cloud storage system. We try to model collusion attack done by revoked users cooperating with existing users. In addition, we construct a competent user revocation Club penguin-ABE plan through increasing the existing plan and prove our plan is CPA secure underneath the selective model. To resolve existing security issue, we embed certificates into each user's private key. In this manner, each user's group secret key differs from others and bound along with his private key connected with attributes. To lessen users' computation burdens, we introduce two cloud providers named file encryption-cloud company (E-CSP) and understanding-cloud company (D-CSP). The job of E-CSP would be to perform outsourced file encryption operation and D-CSP would be to perform outsourced understanding operation. Within the file encryption phase, the operation connected using the dummy attribute is conducted in your area as the operation connected using the sub-tree is outsourced to E-CSP [5]. Benefits of suggested system: Lessen the heavy computation burden on users. We delegate the majority of computation load to E-CSP and D-CSP and then leave really small computation cost to local devices.

**Fundamental Statements:** We are saying that DCDH assumption holds if no probabilistic polynomial time (PPT) adversaries can solve the DCDH trouble with for the most part a minimal advantage. The formula outputs a cipher text so that just the user whose attribute set satisfies the access policy can decrypt. Proxy re-file encryption enables a genuine-but-curious proxy to transform a cipher text encrypted by Alice's public key right into a new cipher text that's able tube decrypted by Bob's

secret key. Within our Club penguin-ABE plan with user revocation, we think that a user's private key includes a double edged sword. The first is connected together with his approved attributes and yet another the first is connected using the group that they is associated with. Within our security model, the revoked users may collude using the existing users within the same group to fight this group and get use of some data. On the other hand, existing users can get private keys that don't fulfill the specific access structure however the version may be the current version.

**Framework:** Each interior node within the access tree is really a threshold gate and also the leave nodes are connected with attributes. A person can decrypt a cipher-text only when his attribute set satisfies the access tree baked into the cipher text. The understanding operation contains two steps. The initial step is the fact that D-CSP performs partial understanding. The 2nd step is the fact that DU decrypts mediate leads to get plaintext. In the following paragraphs, we provided a proper definition and security model for Club penguin-ABE with user revocation [6]. We create a concrete Club penguin-ABE plan that is CPA secure according to DCDH assumption. To face up to collusion attack, we embed certificates in to the user's private key. To ensure that malicious users and also the revoked users don't be capable of produce a valid private key through mixing their private keys. When DO promises to upload his files to CSS and share all of them with you of the specified group, he first defines an access tree and will get the audience public key. During decrypting process, there are plenty of bilinear pairing operations that are computationally costly. To lessen the computation cost, we delegate the pairing operations to D-CSP, around the condition the data submissions are still protected against being uncovered. The primary issue within our plan would be to withstand the collusion attack between your revoked users and existing users [7]. With the introduction of cloud-computing, outsourcing data to cloud server attracts plenty of attentions. To be sure the security and get flexibly fine-grained file access control, attribute based file encryption (ABE) was suggested and utilized in cloud storage system. Furthermore, we delegate operations rich in computation cost to E-CSP and D-CSP to lessen the user's computation burdens. Through using the manner of delegate, computation cost for local devices is a lot lower and comparatively fixed. The outcomes in our experiment reveal that our plan is efficient for resource restricted devices.

#### 4. CONCLUSION:

Our plan is efficient for resource restricted devices for example cell phones. Our plan may be used in cloud storage system that needs the skills of user revocation and fine-grained access control. To lessen users' computation burdens, we introduce two cloud providers named file encryption-cloud company (E-CSP) and understanding-cloud company (D-CSP). The job of E-CSP would be to perform outsourced file encryption operation and D-CSP would be to perform outsourced understanding operation. However, user revocation may be the primary issue in ABE schemes. In the following paragraphs, we offer a cipher text-policy attribute based file encryption (Club penguin-ABE) plan with efficient user revocation for cloud storage system. Thinking about our plan resists collusion attack done by the revoked users cooperating with existing users as the plan doesn't, our plan is much more practical.

#### REFERENCES:

- [1] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc.13th ACM Conference on Computer and Communications Security (CCS '06), pp. 89-98, 2006, doi:10.1145/1180405.1180418.
- [2] M. Green, S. Hohenberger and B. Waters, "Outsourcing the decryption of ABE ciphertexts," Proc.20th USENIX Conference on Security (SEC '11), pp. 34, 2011.
- [3] Z. Liu, Z. Cao, Q. Huang, D. S. Wong and T. H. Yuen, "Fully Secure Multi-Authority Ciphertext-Policy Attribute-Based Encryption with-out Random Oracles," Proc.16th European Symposium on Research in Computer Security(ESORICS '11), LNCS6879, Berlin:Springer-Verlag, pp. 278-297, 2011.
- [4] M. Blaze, G. Bleumer and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography," Proc.International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT '98), LNCS1403, and Berlin: Springer-Verlag, pp. 127-144, 1998.
- [5] J.W. Li, C.F. Jia, J. Li and X.F. Chen, "Outsourcing Encryption of Attribute-Based Encryption with Mapreduce," Proc.14th International Conference on Information and Communications Security (ICICS '12), LNCS7618, Berlin: Springer-Verlag, pp. 191-201, 2012.
- [6] Jiguo Li, Wei Yao, Yichen Zhang, Huiling Qian and Jinguang Han, Member, IEEE, "Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing", IEEE Transactions on Services Computing, 2016.