Simplified ciphertext-policy attribute-based encryption scheme with attribute level collusion resistance for cloud storage

Naresh Vurukonda¹, Venkateshwarlu Velde², M. Trinath Basu³, P. Tejasri⁴

¹, ³Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India.
²Balaji Institute of Technology and Science, Warangal, Telangana, India.
Email: naresh.vurukonda@kluniversity.in

Abstract. The core objective of our paper is that to overcome the challenges of secure data sharing problem in cloud where users can access data if they acquire a certain set of attributes or credentials. At present, there is only one way for implementing such procedures is by employing a reliable server to mediate access control, store the data. The service providers have whole control over cloud applications, client’s data and hardware. However, if the data stored in the cloud server is conceded, then the data confidentiality will be compromised. With simplified CP-ABE data is confidential even though storage server is untrusted. Hence privacy of cloud data is enhanced by proposing a methodology that uses a privacy policy, encrypts the data based upon various group of attributes related to the user. The decryption of the data can be done only when his/her attributes match with the privacy policy. Simplified CP-ABE makes it easier to secure, broadcast and control the access of sensitive information, specifically across the cloud’s server and decrease collision resistance.

Key requirements: Sensitive, Simplified CP-ABE, Privacy Policy, Cloud server, Collision Resistance.

1. Introduction:
Here, the focus is on providing security to the data stored in a cloud. That is taken as primary concern. Generally, the service providers of the cloud have full command on the cloud applications, and they provide the faith and security to customers for storing significant and sensitive data in a great quantity on the cloud. Since it is the central authority based,[¹⁴] the users are unenthusiastic to put their confidential data on cloud as once data is put down in cloud, they may be unable to find their control directly on the data sources.[¹⁸,⁹] Hence cloud requires more secure methods for storing and management to preserve their client’s privacy and data confidentiality.[¹] This is achieved by removing the central authority CSP’s and implementing CP-ABE.

[³]Attribute-based-encryption was proposed by Sahai and Waters in 2005, where ciphertext, keys are related to attributes set and an access policy is specified to decrypt the ciphertext. Since then CP-ABE is commonly used in cloud storage and it’s privacy policy is not good enough as threshold operations can only be achieved. As the cloud storage environment is used by huge number of users, and they may sometimes share a similar attributes, therefore if a user revokes his attribute it has become a problem to give the corresponding users access permissions by not affecting other users access.[²¹] Hence later few scholars proposed ciphertext-policy and key-policy ABE mechanisms. [¹¹] In Key-Policy ABE, user’s credentials are generated based on privacy policy that defines the privilege of specific user, and information is encrypted based on set of attributes.[¹⁶] However, in CP-ABE privacy policy is for encrypting the users information and users keys are created based on the list of attributes. [¹⁵,¹³] In CP-ABE the revocation is achieved by using a binary tree, where the attributes are represented using the tree structure known as access structure. The tree consists of multiple levels, root
node which is the upper most root in the tree, leaf nodes which are the lower-level nodes. It uses a privacy policy which encrypts the information based on several attributes given by the user. If the users given attributes matches with the privacy policy then information can be decrypted by the client. This technique is an enhancement of identity based encryption, which confines access to specific users resulting in faster, secure access to data.

2. Literature Review:
The below mentioned table 1 approaches are identified over the security that simplifies the complexity and provides in depth security through their intended themes:

| S.No. | AUTHOR | TITLE | METHODOLOGY | YEAR |
|-------|--------|-------|-------------|------|
| 1     | [2].Jianhua and Guangbo. | Research on CP-ABE User Revocation on Cloud Storage with Attribute Level Encryption | CP-ABE | 2017 |
| 2     | [3].Sahai Amit Waters Brent John Bethencourt | CP-ABE | Access Control scheme, Cryptography, | 2007 |
| 3     | [4].Dr.Rashmi Rach,Sneha Chandrashekhar | CP-ABE | CP-ABE | 2017 |
| 4     | [5].V.Naresh, B.Tirumala Rao | DC-MAABE Data Centric Multi ABE on Cloud Storage. | DC-MAABE | 2019 |
| 5     | [6].Waters.B | CP-ABE with anonymous access policy | CP-ABE | 2008 |

Table 1: Existing Approaches over the proposed theme

3. METHODOLOGY:
As depicted in Figure 1 CP-ABE consists of 4 steps.

```
BLOCK DIAGRAM

CP-ABE SETUP --> KEY GENERATION --> ENCRYPTION --> DECRYPTION
```

Figure 1: Block Diagram for Simplified CP-ABE

3.1 Setup:
After successful installation of simplified cp-abes. [3,7,16] The setup algorithm generates two keys namely a master key (MK) and public key(PK).
3.2 Generation of Key:
In key generation a key generated called private key(PVK) by taking input as the set of attributes[22]. The Attributes can be in numeric or non numeric formats .Non-numeric means collection of letters, underscores and numbers. Some examples of attributes are student ,name ,age.

3.3 Encryption:
Encrypts a file such as text document, Based on the user attributes we create a privacy policy (PP).[3,12,19] Privacy policy consists of AND and OR Operations along with the group of attributes as depicted in Figure 2.

![Figure 2](image_url)

**Figure 2.** The Above figure is the privacy policy access structure which uses ‘and' and ‘or’ operators.

3.4 Decryption:
Decryption of a file such as text document ,Using the privacy policy . [8,10] The encryptor can be able to encrypt the file only when attributes given by the users satisfy the privacy policy.

4 .RESULTS & DISCUSSIONS:
For the simplified cp-abe implemetation we need to download cpabe-0.11, libbswabe-0.9, pbc-0.5.14, gmp-6.2.0
Commands:
➢ cd gmp-6.2.0 // change directory
➢ ./configure // configuring
➢ Make    // make commit
➢ Make check // make check
➢ Sudo make install // root

The above commands are needed to be followed for all the four files.
For the genaration of master key(MK) and public key(PK) we need to run cpabe-setup as shown in Figure 3 .We created a folder named klu and we stored the generated master key and public key into the klu folder.
Tejasri and Tejaswi are the two users who are using cloud environment for storing their data. Based on different set of user attributes private keys are generated as shown in Figure 4. Tejasri attributes are student, cse_department and id number and Tejaswi attributes are klu_student, cyber_security, id number keys are generated based on the information given by the users.

```bash
tejasri_priv_key:
$ cpabe-keygen -o tejasri_private_key public_key master_key
  student cse_dep 'id = 170030991' 'joining_date = `date +%s`

tejaswi_priv_key:
$ cpabe-keygen -o tejaswi_private_key public_key master_key
  klu_student cyber_security 'cgpa = 8'
  'id = 170030992' 'joining_date = `date +%s`
```

**Figure 3. cpabe-setup**

**Figure 4. Private Key Generation**

### 4.1 Privacy Policy:
[1,17] As shown in Figure 5 Privacy Policy is for encrypting the files that are confidential and needs security. klu.txt is the file that we have encrypted as shown in Figure 6. Based on the users attributes such as tejasri and tejaswi the privacy policy is created.

```
cpabe-enc pub_key klu.txt
(student and (joining_date< 946702800 or focus_cse)) or
(klu_student and 2 of (cgpa>= 6, cse_team, cyber_security))
```

```bash
cpabedec pub_key klu.txt
```
Figure 5. Privacy Policy

Figure 6. Cpabe-Encryption

cpabe-dec pub_key tejaswi_priv_key klu.txt.cpabe
Tejaswi attributes satisfy the privacy policy so the decryption of the klu.txt file is done as shown in Figure 7.

cpabe-dec pub_key tejasri_priv_key klu.txt.cpabe
Tejasri attributes do not satisfy the privacy policy so she will not be able to decrypt klu.txt file and she will get an error 'cant read the file' as shown in Figure 7.
The following is the graph that shows performance of the encryption that is used in this theme.

![Graph showing performance of encryption](image1)

**Figure 7. Cpaeb- Decryption**

The above shown graph tell us about the encryption time based on attributes number. As shown in Figure 8, as the attributes number increases encrypting time will be increased.

![Graph showing encryption time vs number of attributes](image2)

**Figure 8. Encryption time Vs No of attributes graph**
The above shown graph tells us about the decryption time depending on attributes number. As seen in Figure 9, as the attributes number increases decryption time will be increased. Compared to previous scheme our scheme gives lower decryption time.

5. Conclusion:
As security is the basic need of cloud users since they store their important personal information in the cloud server. Through our simplified CP-ABE the privacy of cloud data is increased by using the good seamless user privacy policy mechanism. Here collision resistance can be achieved by the client who can only satisfy the privacy policy and could decrypt the confidential information which requires security. This system allows access control of encrypted information where private keys of the user are generated by given group of attributes and data encryption that state a policy across the attributes that decryption can be done by the user. This system allows policies as unique access tree structure and where attacker may acquire different private keys it is collision resistant. The system implementation we had given includes various methods for optimization.

References:
[1] Q. Wang, L. Peng, H. Xiong, J. Sun and Z. Qin, "Ciphertext-Policy Attribute-Based Encryption With Delegated Equality Test in Cloud Computing," in IEEE Access, vol. 6, pp. 760-771, 2018, doi: 10.1109/ACCESS.2017.2775741.
[2] Guangbo Wang, Jianhua Wang, "Research on Ciphertext-Policy Attribute-Based Encryption with Attribute Level User Revocation in Cloud Storage", Mathematical Problems in Engineering, vol. 2017, Article ID 4070616, 12 pages, 2017. https://doi.org/10.1155/2017/4070616.
[3] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in 2007 IEEE Symposium on Security and Privacy (SP '07), Berkeley, CA, 2007 pp. 321-334, doi: 10.1109/SP.2007.11.
[4] Sneha Chandrashekhar Parit, Dr. Rashmi Rachh, "Ciphertext Policy Attribute Based Encryption" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 04 Issue: 04 , Apr-2017.
[5] Vurukonda, Naresh, and B. Thirumala Rao. "DC-MAABE: Data Centric Multi-Authority Attribute Based Encryption on Cloud Storage." Journal of Computational and Theoretical Nanoscience 16.5-6 (2019): 1893-1901.
[6] Waters, B.:”Ciphertext-policy attribute-based encryption”: An expressive, efficient, and provably secure realization. Technical report, SRI International (2008) (to appear).
[7] Yadav, Umesh Chandra, and Syed Taqi Ali. "Ciphertext policy-hiding attribute-based encryption", 2015 International Conference on Advances in Computing Communications and Informatics (ICACCI), 2015.
[8] Brent Waters. "Attribute-based encryption with non-monotonic access structures", Proceedings of the 14th ACM conference on Computer and communications security - CCS 07 CCS 07, 2007.

[9] R. Gavriloae, W. Nejdl, D. Olmedilla, K. E. Seamons, and M. Winslett. No registration needed: How to use declarative policies and negotiation to access sensitive resources on the semantic web. In ESWS, pages 342–356, 2004.

[10] Michel Abdalla, Dario Catalano, Alexander W. Dent, John Malone-Lee, Gregory Neven, and Nigel P. Smart. Identity-based encryption gone wild. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors.

[11] Changji Wang, Jianfa Luo, "An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length", Mathematical Problems in Engineering, vol.9 2013, Article ID 810969, 7 pages, 2013. https://doi.org/10.1155/2013/810969.

[12] Vanraj Kamlia, Rajnikanth Aluvalu, “A Survey on Hierarchical Attribute Set based Encryption (HASBE) Access Control Model for Cloud Computing.” International Journal of Computer Applications (0975 – 8887) Volume 112 – No. 7, February 2015.

[13] Vurukonda Naresh, B. Thirumala Rao, and B. Tirapathi Reddy. "A Secured Cloud Data Storage with Access Privilege" (IJCE) (2016): 2338-2344.

[14] B. Thirumala Rao, and L. S. S. Reddy. “Survey on improved scheduling in Hadoop MapReduce in cloud environments.” arXiv preprint arXiv:1207.0780 (2012).

[15] Wei Teng, Geng Yang, Yang Xiang, Ting Zhang, and Dongyang Wang. “Attribute-based access control with ciphertext in cloud computing”. IEEE Transactions on Cloud Computing, (2017).

[16] Umesh Chandra, Syed Taki “Ciphertext policy-hiding attribute-based encryption” International Conference on Advances in Computing, Communications and Informatics (ICACCI).

[17] Helli K. Rahman “CP-ABE Access Control Scheme for Sensitive Data Set Constraint with Hidden” Access Policy and Constraint Policy” College of Mathematics and System Science, Xinjiang University, Xinjiang, N China (2017).

[18] S. Subashini, V. Kavitha, “A survey on security issues in service delivery models in cloud computing”. J. Netw. Comput. (2011).

[19] R Ostrovsky, “Attribute based encryption using non monotonic access structures.” CCS ’07 Proceedings of the 14th ACM conference on Computer and communications security.

[20] Prashant, A. Kadam, Avinash Devare,"A Secure, Scalable, Flexible and Fine-Grained Access Control Using Hierarchical Attribute-Set Based Encryption in Cloud Computing.” International Journal of Computer Applications Technology and Research Volume 3– Issue 12, 799 - 808, (2014).

[21] Anup R. Nimje, V. T. Gaikwad, H. N. Datir, “Attribute-Based Encryption Techniques in Cloud Computing Security : An Overview.” International Journal of Computer Trends and Technology- volume4 (2013).

[22] Fuchun Guo, Yi Mu, Willy Susilo, Duncan S Wong, and Vijay Varadharajan. Cp-abe with constant-size keys for lightweight devices. IEEE transactions on information forensics and security, 9(5):763–771, 2014.