International Journal of Engineering & Technology, 7 (4.6) (2018) 1-3

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Fine Grained Access Control Policy with Advanced Encryption Standard in the Cloud Computing

Krishna Keerthi Chennam[1]*, Lakshmi Muddana[2]

[1]*Research Scholar,Gitam School of Technology, Hyderabad*
[2]*Prof and IT HOD, Gitam School of Tehcnology,Hyderabad*
**Corresponding author E-mail: krishnakeerthich@gmail.com*

Abstract

The Data Base as a Service is a great example where the database engine and storage devices are in cloud data. This scheme allows customers to outsource data and store in cloud database on pay per user, scalable and flexible. But data confidentiality is in high risk when data is outsourced and stored in third party database. A trusted third party server must be maintaining the third party data base. There is a possibility of malicious administrator who can leaks the data which is stored in third party database. The best method is to encrypt the data and store in third party database but alone encryption is not sufficient. Even authorization is another problem that who can access the data. For data security and authorized of users, the fine grained access control policy Cipher text policy Attribute Based encryption (CP-ABE) is used to give access to authorized users only and the best symmetric encryption Advanced Encryption Standard(AES) is applied on data before outsourcing the data in cloud.

Keywords: *CP-ABE; AES; Cloud Data Base; Data Security; Access Control Policy.*

1. Introduction

A new emerging technology is cloud with different internet server maintains the owner data in the cloud [1][2][3], where third party is a untrusted server and database, the access control and confidentiality of the secure data is the main problem in the cloud server [4][5]. Data owners are afraid to outsource the data to store in third party server because of security problems. The access control policy authenticates the authorized users and permits access to the data [6] [7] [8]. Focusing on two threats[9][10], Firstly the users tries to retrieve data must be authorized users, access control is given based on the ABE [11] where there are different ABE control policies to prevent the malicious users to access the private data. The data owner maintain the attribute set and based on the attribute set of the users must match with the data owner set with AND and OR logic gives authentication to the authorized users only to access the data. Secondly the outsourced data must be secure by encrypting the plain data before storing in cloud database using AES symmetric encryption. If any malicious third party server or malicious admin tries to leak the data from the third party database. The data is encrypted before outsourcing the data in cloud with symmetric AES encryption technique. Symmetric encryption is the fast and flexible encryption technique to secure the data.

2. Related work

There are different existing access control policies that provide secured access to the users with the ABE. Initial property of ABE is hindering against user fraudulent. Main purpose of the ABE to give security and access control. The encryption technique is public key encryption which allows users to encrypt and decrypt data based on the attributes of users. ABE is developed based on the Identity Based encryption (IBE) where IBE uses only one attribute to identify the user. ABE [12] uses the multiple attributes with access control policy.

2.1. Attribute Based Encryption (ABE)

ABE provides the unacknowledged access control, keys generated based on the attributes to convert into cipher text. The users who are authorized get keys to decrypt a cipher text when user attributes matches with the data owner where there is minimum required threshold attributes should match with the user ABE important feature collusion resistance. It users tree based access structures. The drawback of ABE is the data owner required the user public key where the data encrypts for every access.

2.2. Cipher text Policy -ABE

Attribute set is accomplice with private users in KP-ABE. Data owner encrypts the plain text to cipher text with accomplice access policy with the cipher text. To give access to the data the user must satisfy the access structure. The access structure is designed with AND, OR logics. User decrypts the data when user attributes satisfy the access structure which is combined with cipher text. Most of the ABE's are derived from CP-ABE [13] [14] only. Multiple sets are not acceptable in CP-ABE.CP-ABE derived from KP-ABE and give access to select the key who can recover the data. Encryptor has rights to take decision in granting permissions to the decryptor.

CP-ABE has 4 steps algorithms:

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Setup: CP-ABE takes input as a security K, Public key PK, with master secret key MSK, users require PK to encrypt .MSK is used for users secret key where authorize user only able to know.

Encrypt: Message M, Public key PK, Access Structures AT, gives output as Cipher Text CT.

Key-Gen: Keys are generated are based on the all attributes set and Master secret key MSK. Output is a Secret Key SK with the users attribute structure.

Decrypt: Input is a Cipher Text CT and Secret Key SK with set of attributes gives the Plain Text M.

CP-ABE tries to overcome the problems in ABE by giving access to encryptor where encryptor can select the decryptor who matches with attribute set. Disadvantage of CP-ABE is not flexible user should satisfy the access attribute set then only user will get key to decrypt the Cipher Text.

2.3. Bilinear Maps

Definition: Tow cyclic groups with prime order p are G_1, G2 mapping e: G1 × G_2 →G_2, where G_1 is a bilinear group if

1. For all u,v ϵ G, and a,b ϵZ_p, we have $e(u^a,v^b)=e(u,v)^{ab}$
2. $e(g,g) \neq 1$;
3. Both G_1, e are efficient.

2.4. Advanced Encryption Standard (AES)

In [17] AES is notorious and large number of users are utilize symmetric encryption algorithm. AES is fixedly symmetric block cipher and has variable key sizes with 128,192 and 256 bits compared to DES. AES is alike to replacement which is restored inputs by the outputs and the transformation is shamble bits. AES enforce utter operations on bytes by converting bits. AES designed plain text of 128 bits as 16 blocks, 4 columns array and 4 rows as matrix. Rounds are assorted based on the key size of 128 bits has 10 rounds, 192 bits has 12 rounds and 256 bits has 14 rounds.

Encryption: Every round has 4 sub processes as shown below Fig. 1.

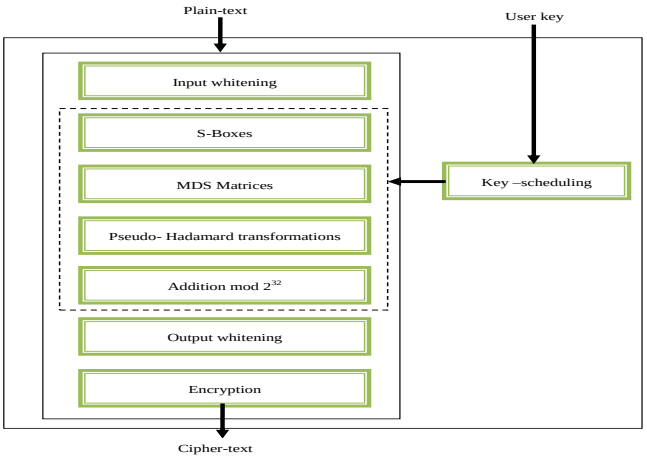


Fig. 1. Sub Process of AES

Sub Bytes: S-Box is the substitution of bytes as the input 16 bytes which gives 4 rows and 4 columns matrix.

Shift rows: Second row is shifted to the first position to the left. Third row shifted left by two positions. Fourth row shifted left by 3 positions. Result is the new matrix with 16 bytes.

Mix Columns: Each column of 4 bytes as input and new bytes as output which give new matrix with 16 bytes.

Add round key: The 16 bytes acknowledge as 128 bits and XORed the 128 bits. The output is taken as cipher text in the last round, aside from one more time consider this output as succeeding round input and rerun the process until completing the rounds.

Decryption: AES decryption is similar to encryption as reverse order with rounds each round contains Add round key, mix columns, shift rows, Byte substitution which gives output as plain text in last round. Advantage of AES is the flexibility in key size and competency to give keys with good management.

3. Proposed Method

Dealing with a sensitive data and storing on cloud increases the risk of authentication of users and the malicious or curious administrator. The proposed work as shown in fig. 1. includes authentication of users by including the fine grained access control policy CP-ABE, where in CP-ABE the data owner provides the attributes set ,who ever user tries to access the data should match the attributes set and have the key to decrypt the data, where the encryptor provides the key to the user based on the access control policy[18]. The data is encrypted before outsourcing the data on cloud with symmetric encryption using AES, where the curious or malicious administrator cannot leak data when that data is in encrypted form and administrator does not have the key to decrypt the data. By using this proposed method CP-ABE with AES encryption technique the data owner feels the data is secured with the AES encryption and authentication provides with the CP-ABE access control policy. By comparing the CP-ABE with Bilinear [16] and CP-ABE with AES in different parameters as shown in table 1. Cipher text description and private key descriptions are associated with the policy over key attributes in both CP-ABE with bilinear mapping and CP-ABE with AES. The position of attribute description is given by the client in both methods. Access policy and Initiative of access control is given by the server in both existing and proposed methods. The key generation time is gradually reduced compared with the existing method, CP-ABE with bilinear mapping has high key generation time than the CP-ABE with AES. The plain text is encrypted before outsourcing the data in cloud to secure the data from the malicious administrator, the encryption time is reduced in CP-ABE with AES when compared with CP-ABE with bilinear mapping and KP-ABE. The client need to decrypt the data, the decryption time is reduced when compared with the CP-ABE with bilinear mapping and KP-ABE than the CP-ABE with AES. Cipher text size is linear and security is high in both proposed and existing methods.

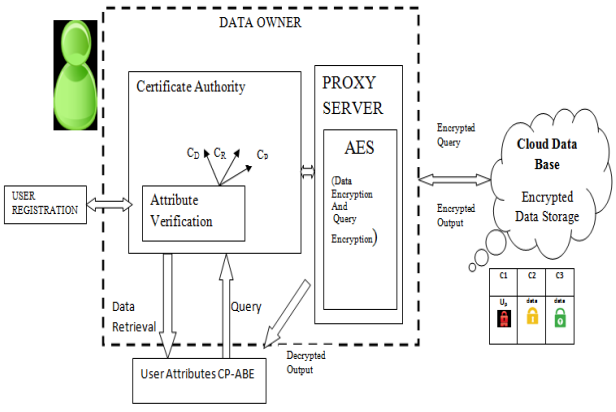


Fig. 2. Block diagram of proposed methodology

Table I. Comparison of CP-ABE Schemes.

Parameter	Comparison of Bilinear and AES with CP-ABE	
	CP-ABE with bilinear mapping	CP-ABE with AES
Cipher text description	Associated with policy over attributes	Associated with policy over attributes
Private key description	Associated with set of attributes	Associated with set of attributes

Position of attribute description	Client	Client
Position of access policy	Server	Server
Initiative of access control	Server	Server
Key generation time	High	Lower than CP-ABE with bilinear mapping
Record access time	High	High
Encryption Time	Lower than KP-ABE	Lower than CP-ABE with bilinear mapping
Decryption time	Lower than KP-ABE	Lower than CP-ABE with bilinear mapping
Cipher text size	Linear	Linear
Security	Fully secure	Fully secure

The proposed method provides security to the records in cloud domain. By using the estimation metrics of key generation time and encryption time the attainment of the selected system is evaluated. The key generation time is calculated based on the number of attributes in the private key and time to generate private key in ms. The time to generate private key in CP-ABE with AES is less than the CP-ABE with Bilinear mapping as shown in graphs. It is clear that for 10 number of attributes the time take to generate private key is 0.2 ms, for 20 attributes the time taken is 0.5 ms, for 30 attributes the time taken is 0.8 ms, for 40 attributes the time taken is 1.2 ms, for 50 attributes the time taken is 1.5 ms respectively as shown in Fig. 3.

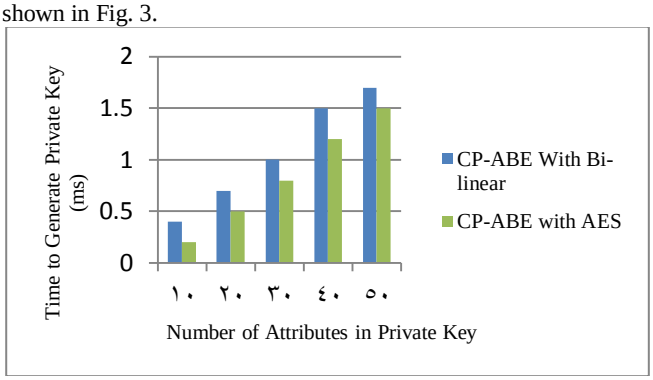


Fig. 3. Key Generation time in CP-ABE with Bilinear Vs CP-ABE with AES

The data stored in cloud is encrypted, the encryption time is calculated based on the number of leaf nodes in the policy and time to encrypt in ms. The time to encrypt data in CP-ABE with AES is less than the CP-ABE with Bilinear mapping as shown in graphs. It is clear that for 20 number of leaf nodes in policy the time taken to encrypt the data is 0.2 ms, for 40 leaf nodes in policy the time taken is 0.8 ms, for 60 leaf nodes in policy the time taken is 1.3 ms, for 80 leaf nodes in policy the time taken is 1.8 ms and for 100 leaf nodes in policy the time taken is 2.4 ms respectively as shown in Fig. 4.

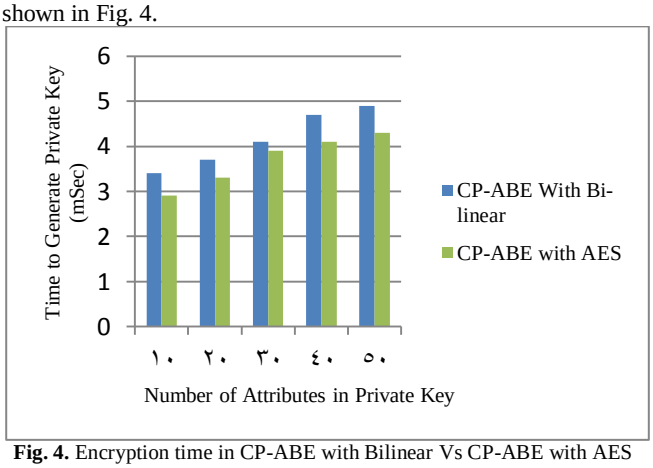


Fig. 4. Encryption time in CP-ABE with Bilinear Vs CP-ABE with AES

4. Conclusion

To give privacy and security for data records the data is encrypted and stored in cloud data base and give access to the user based on the key policy generated by the data owner. The data owner gives the number of attributes and creates the policy based on the attributes the client get access to data and store the data. The private key is shared based on the access control policy. To secure the data is encrypted and stored in cloud. The proposed CP-ABE with AES provides the less key generation time and encryption time when compared with CP-ABE with Bilinear mapping as shown in results .In future by using various encryption techniques to secure the data records.

Acknowledgement

I acknowledge my sincere gratitude towards my guide who helped me in publishing paper in this journal.

References

[1] A.Behl, "Emerging Security Challenges in Cloud Computing: An insight to cloud security challenges and their mitigation", word congress on Information and Communication Technologies,2011, PP. 217-222.
[2] M. Peter and G. Tim. The NIST Definition of Cloud Computing. National Institute of Standards and Technology, 53(6):50, 2009.
[3] Z. Xiao and Y. Xiao, Security and privacy in cloud computing. Communications Surveys Tutorials, IEEE, PP(99):1 –17, 2012.
[4] A.B. Lewko et al, ''New Proof Methods for Attribute-Based Encryption: Achieving Full Security through Selective Techniques,'' in Proc. 32st Ann. Int'l Cryptology Conf.: Advances in Cryptology - CRYPTO'12, Vol. 7417, pp. 180-198,2012.
[5] Shucheng Yu, Cong Wang, KuiRen, Wenjing Lou - Attribute based data sharing with attribute revocation. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, pp. 261- 270, 2010.
[6] S. Narayan, M. Gagné, R. Safavi- Naini, "Privacy preserving EHR system using attribute-based infrastructure", In Proceedings of the ACM workshop on Cloud computing security, pp. (47-52), 2010.
[7] K. Yang and X. Jia, "Attributed-based access control for Multi authority systems in cloud storage", in Distributed Computing Systems (ICDCS), 2012 IEEE 32nd International Conference on, 2012, pp. 536–545.
[8] J. Bethencourt, A. Sahai, and B. Waters, Cipher text policy attribute based encryption, in Proceeding IEEE Symposium Security and Privacy, 2007
[9] Ryan M.D, "Cloud computing privacy concerns on our doorstep", Communications of the ACM, Vol. 54, No.1, pp.36–38, 2011.
[10] Ryan M.D, "Cloud computing security: The scientific challenge, and a survey of solutions", Journal of Systems and Software, Vol.86, No.9, pp.2263-2268,2013.
[11] Amit sahai and Brent Waters," Fuzzy identity-based encryption", In advances in cryptology EUROCRYPT 2005,pp 457-473.
[12] Allison Lweko,Amit Sahai, and Brent Waters," Revocation systems with very small private keys", In IEEE Symposium on Security and Privacy,2010, PP 273-285.
[13] Brent Waters," Cipertext-policy attribute based encryption:An expressive efficient, and provably secure realization", In Public key Cryptography-PKC 2011,pp53-70
[14] Xieming Liu, JinboXiong, "Ciphertext-Policy Weighted Attribute Based Encryption for Fine-Grained Access Control", 5th International Conference on Intelligent Networking and Collaborative Systems (INCoS), 2013.
[15] Qinyi Li, Hu Xiong, and Fengil Zhang," Broad cast revocation scheme in composite order bilinear group and its application to attribute based encryption . International Journal of Security and Networks,2013,pp 1-12.
[16] C.H.Liu,F.Q.Lin,C.S.Chen,T.S.Chen,"Design of secure access control scheme for personal health record based cloud health care service", Security and Communication Networks,2015,Vol.8,No.7,pp.1332-1346.
[17] Rijmen V, Daemen J. Advanced encryption standard. Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology. 2001:19-22.
[18] Samarati P, De Capitani di Vimercati S. "Data protection in outsourcing scenarios: issues and directions." In: Proceedings of the 5th ACM Symposium on information, computer and communications security (ASIACCS). ACM; pp. 1e14, 2010.