PRIVACY AND OWNERSHIP PROTECTION OF OUTSOURCED CLOUD DATA

Yogita Sharad Deshmukh

M.E.Computer Engineering, Matoshri College of Engineering and Research Center, Maharashtra , India

ABSTRACT

Cloud computing is emerging technology for data storage .The user can store and share the documents using the cloud storage. Hence data security and ownership are critical concerns in cloud computing . It is common nowadays for data owners to outsource their data to the cloud. Since the cloud cannot be fully trusted, the outsourced data should be encrypted .Attribute based encryption (ABE) schema is used. But standard ABE scheme has large cipher text size and high decryption cost, and this problem is especially for resource limited devices such as mobile devices. So we design an ABE scheme for a secure cloud storage service By allowing a third party to achieve a data privacy, integrity.aslo asymmetric algorithms (RSA, AES, and Deffie hellman) are applied to a cloud computing model to ensure the data security. Proposed system reduces the ciphertext size and decryption time using RCCA standard,also prove ownership of data in cloud by using Tag generation algorithm and hash algorihm.

Keyword : - *Data Security,Ownership,Attribute based encryption, outsourced decryption.*

1. Introduction

Cloud computing is an emerging technologies in recent years. It is an application or service that runs on a distributed network .Cloud services allow individuals to use software and hardware that are managed by third parties at remote locations. Cloud services include online data storage, social networking sites, webmail, and online business applications. Cloud computing can reduce the cost and complexity of the networks and other benefits to users include scalability, reliability, and efficiency.

Cloud computing intensifies the Information Technology (IT) architecture with the following advantages: on-demand self-service, resource elasticity, and shared pool access. The objective of cloud paradigm is to share the data computations over the scalable network nodes, namely, user computers,cloud services, and data centers. Several grades of services are available in the cloud architecture,namely, SoftwareAsAService (SAAS), Platform As A Service (PAAS), and InfrastructureAsAService (IAAS)

As many companies, organizations outsourced their sensitive data to the cloud, Therefore Cloud service provider should provide the trust and security, as there is valuable and sensitive data in huge amount stored on the clouds. For protecting the confidentiality of the stored data, the data must be encrypted before uploading to the cloud by using some special cryptographic algorithms. . Computer based security measures mostly capitalizes on user authorization and authentication. In traditional encryption schemes, a sender usually needs to know the identities of the intended recipients and needs to pre-share credentials with them. The objective is that a sender encrypts data that can only be decrypted and read by an exact recipient. Given its exclusive benefits, ABE has recently gained much attention and has been adopted by many cloud computing applications and large-scale dynamic systems. The concept of ABE was first introduced by Sahai and Waters [1] Attribute-based encryption (ABE) is an expansion of public key encryption that allows users to encrypt and decrypt messages based on user attributes.There are two kinds of ABE having been proposed: Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE). In KP-ABE, the access policy is assigned in private key, whereas, in CP-ABE, it is specified in ciphertext. Recently, as the development of cloud computing, users concerns about data security are the main obstacles that impedes cloud computing from widely adopted. These concerns are originated from the fact that sensitive data resides in public cloud, which is maintained and operated by untrusted Cloud

Service Provider (CSP). ABE provides a secure way that allows data owner to share outsourced data on untrusted storage server instead of trusted server with specified group of users. This advantage makes the methodology appealing in cloud storage that requires secure access control for a large number of users belonging to different organizations.

Nevertheless, one of the main efficiency drawbacks of ABE is that the computational cost during decryption phase grows with the complexity of the access formula. Thus, before widely deployed, there is an increasing need to improve the efficiency of ABE. To address this problem, outsourced ABE, which provides a way to outsource intensive computing task during decryption to CSP without revealing data or private keys, was introduced [2][3]. It has a wide range of applications.

2. Literature Survey

Literature survey includes study of Different schemes in Attribute Based encryption (ABE). That are KP-ABE, CP-ABE, Attribute-based Encryption Scheme with Non-Monotonic and Access Structures.

2.1 Attributed Based Encryption

Sahai and Waters in 2005[1] introduced attribute based encryption scheme and the aim of this scheme is to provide security and access control. Attribute-based encryption (ABE) is an one to many encryption based on public-key. The encryption and decryption of the data is based on attributes of the user. The secret key of both the user and the encrypted text are depends on the attributes. The decryption is possible only if the attributes set of the user key matches the attributes of the encrypted text. In ABE(Attribute-based Encryption) scheme, attributes play a very important role [2]. To generate a public key for encrypting data the attribute is exploited and is used as an access policy to control users' access. The access policy can be classify as either key-policy or ciphertext-policy. The key policy is the access structure on the user's private key, and the ciphertext-policy is the access structure on the ciphertext.

2.2 Key Policy Attribute Based Encryption (KP-ABE)

V. Goyal, O. Pandey, A. Sahai, and B. Waters [3] introduced a key-policy attribute-based encryption (KP-ABE) scheme. The modified form of classical model of ABE is KPABE. An access tree structure over the data attributes are assigned to the users. The nodes of the access tree are the Threshold gates. The attributes are associated by leaf nodes. The private key of the user is defined to reflect the access tree Structure. Sets of attributes are labeled with the ciphertexts and private keys are associated with monotonic access structures. These access structures are used for identifying which ciphertexts a user is able to decrypt.Ostrovsky et al. [14] proposed a KP-ABE scheme that allows a user's private key to be expressed in terms of any access formula over attributes. Okamoto and Takashima [12] proposed KP-ABE and CP-ABE schemes with nonmonotone access structures.

2.3 Cipher Text Policy Attribute Based Encryption

CP-ABE scheme was introduced by Sahai [4]. In a CP-ABE scheme, each ciphertext is associated with an access policy on attributes. Every users private key is associated with a set of attributes. The set of attributes associated with the user's private key must satisfy the access policy associated with the ciphertext. Then only a user could decrypt a ciphertext. CPABE works in the reverse mode of KP-ABE. It inherits the same access structure which was used in KP-ABE. Lewko et al .[7] proposed a fully secure CP-ABE scheme. In [11], Waters proposed several very efficient CP-ABE constructions

2.4 Hierarchical attribute based Encryption

Wang et al [13] proposed the Hierarchical attribute-based encryption (HABE) scheme. ABE model consists of a root master (RM), third trusted party (TTP), multiple domain masters (DMs) and numerous users. The root master corresponds to the third trusted party (TTP), the top-level DMs in the multiple domain masters correspond to

multiple enterprise users, and all personnel in an enterprise correspond to the users. In HABE scheme the keys are generated using the property of hierarchical generation of keys in HIBE**.**

3. Proposed Method

[1]. Fig.1 shows the detail architecture of the system

Firstly user store file on cloud storage in encrypted form .By third party auditor mobile user can access the cloud storage data easily. Proposed system is design for, to prove ownership of data in cloud because Ownership means that you can prove complete control of your sensitive data. To prove ownership hash algorithm and tag generation algorithm is used in the design as follows :

Firstly user outsourced data on cloud storage in encrypted form using AES algorithm.

a) The input file 'F' is divided into number of blocks and calculates number of blocks 'B' i.e F=(B1,B2,……Bn).

b) For each block calculate hash function and tag generation algorithm for ownership as follows

TAG(F)=Crate unique tag TAG for file and save in local storage.

TAG(Bn)=Create Tag for each block i.e unique hash value for each bloack

c) For all block calculate Total hash value i.e (blockhash%2==0)

d) Calculate total hash for all block into single hash.

Filehash=H(H(B1)||H(B2)||H(Bn))

e) Then,File data uploaded on server with(file,filehash,ownership hash,file pointer,Encryption key value) to server

[2]. The proposed system presents a android mobile phone application for accessing the cloud database though the third party auditor named.The application contains following functions.

a. Dataset Details : Gives stored database details

b. K-means Clustering:

c. TF –Calculations : Shows term frequency Calculation

d. SQL Query :For sending SQL query like insert,update,delete

e. Featch SQL Record –Display all records

f. Amazon EC2 Website-Is a Third party server.

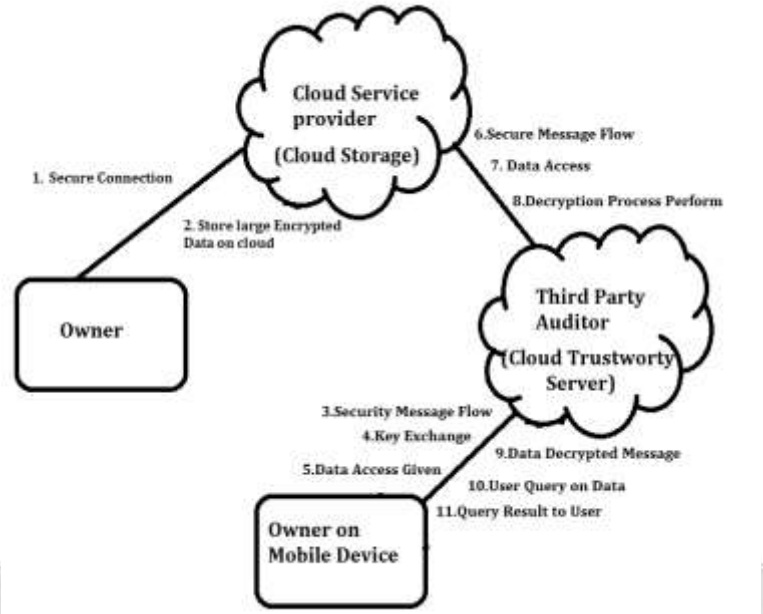


Fig -1: Architecture of proposed system

4.MATHEMATICAL MODULE

Let, S= {I, E, O, D
Where,
S= S can be defined as system.
I=Represents set of input Data I= $\{I_1, I_2 \ldots\ldots I_n\}$
O=Represents set of output data O= $\{O_1, O_2 \ldots\ldots O_n\}$
E=E is the encryption algorithm (AES Encryption Algorithm)$\{E_1,E_2,\ldots E_n\}$
ABE=ABE is attribute based encryption on data E
U_c= User login details of parse cloud
A_z=Amazon cloud details of user login
A_k=AES user encryption key
D=Represents set of decrypted data $\{D_1, D_2 \ldots D_n\}$
Q=Represents user query $\{Q_1, Q_2,\ldots Q_n\}$
R=Represents set of result generated from user query $\{R_1, R_2 \ldots R_n\}$

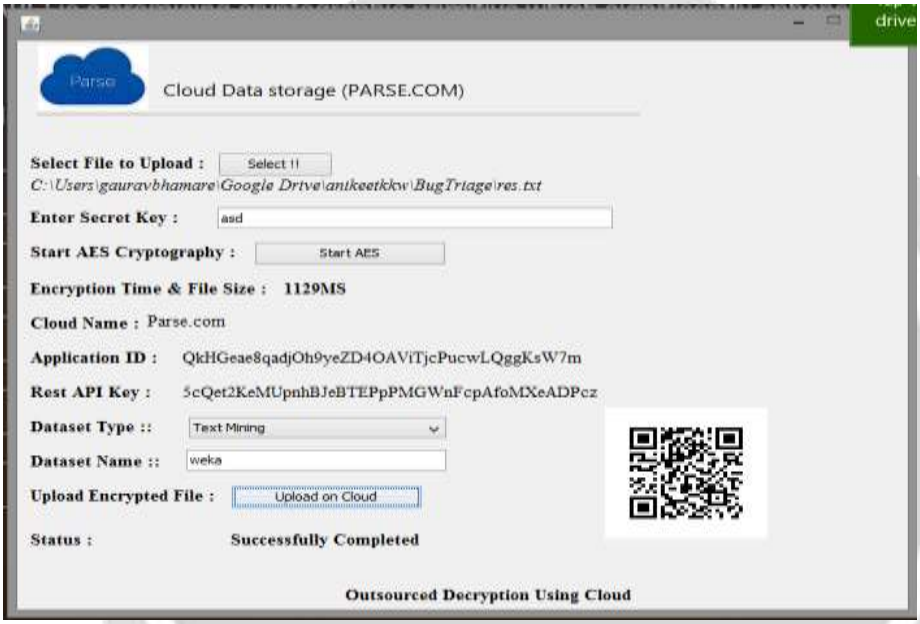
a) Function f1-This function reads the user data and apply AES Encryption on it
$F_1(D) \rightarrow \{(D_1, D_2 \ldots D_n) \rightarrow E\} \varepsilon \{E_1,E_2,\ldots E_n\}$
b) Function F2-This function read user details and Insert this data on cloud service provider.
$F_2(E) \rightarrow \{(\{E_1,E_2,\ldots E_n\}) \rightarrow cloud\{Inert\}\}$
c) Function F3-This Function gives cloud service provider access to third party cloud for processing .
$F_3(User\ Access) \rightarrow \{U_c \rightarrow (A_Z)\}$
d) Function f4-This function send user AES key to third party service provider
$F_4(A_k) \rightarrow \{(A_k \rightarrow A_z)\} \varepsilon A_z$
e) Function F5-This Function download User data from cloud service provider and Perform Decryption on it.
$F_5(A_z) \rightarrow \{(E_1,E_2,\ldots E_n) \rightarrow D)\} \varepsilon \{D_1, D_2 \ldots D_n\}$
f) Function F6-In this Function User Request Query is send to the third party cloud for processing
$F_6(Q) \rightarrow \{(Q_1, Q_2,\ldots Q_n) \rightarrow \{To\ third\ party\ cloud\}\}$
g) Function F7- In this function third party cloud apply attributes based encryption algorithm on data D and select user related access attribute only

$F_7(ABE)->\{(ABE)->\{A_1,A_2,A_3....A_K\} \ \varepsilon \ A\}$
K=K is the selected attribute
n=n is the total no of attribute
K<n

h) Function f8-This Function send computed result to user.
$F_8(D,K,ABE)->\{R \ \varepsilon \ (R_1, R_2 \ ....R_n)\}$

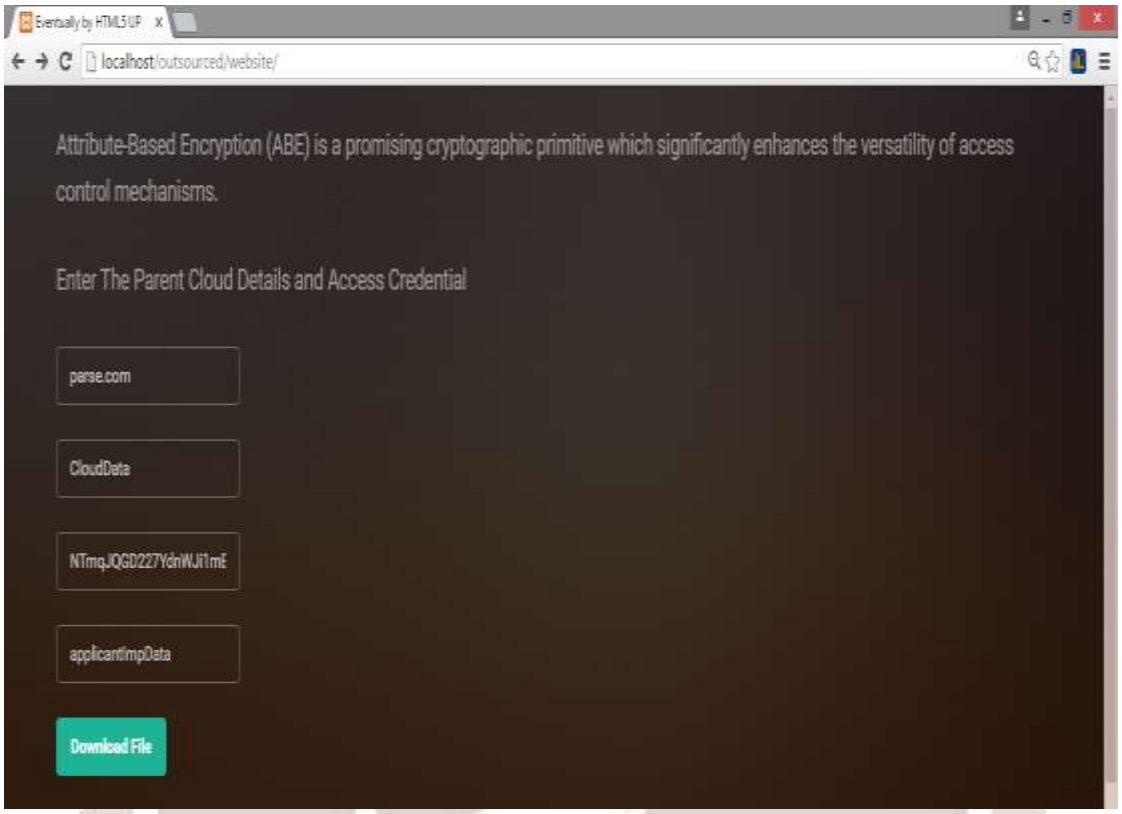
5. EXPERIMENTATION AND RESULT

1. File upload on cloud storage (i.e on Parse.com)



2. Mobile User Cloud Data base application

3. Attribute Based Encryption for decrypt outsourced decryption.



6.RESULTS

1. Table 1: shows Data Encryption using AES and Cloud Upload

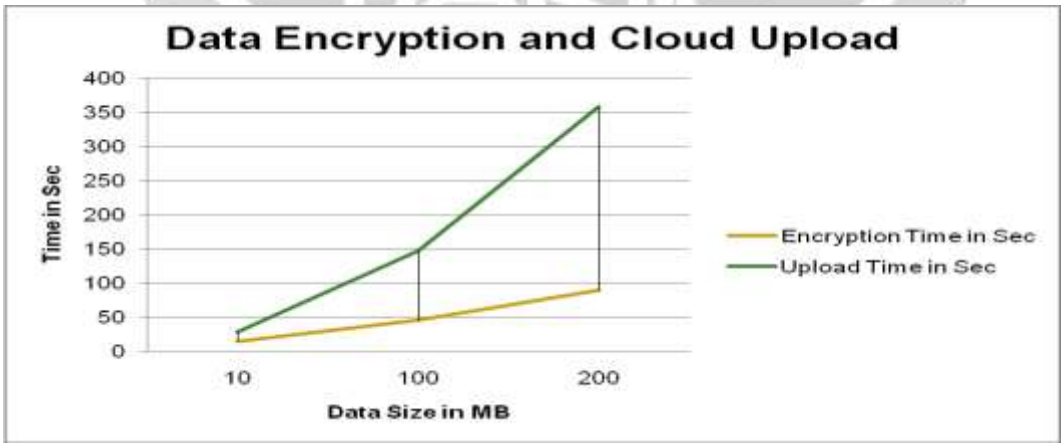
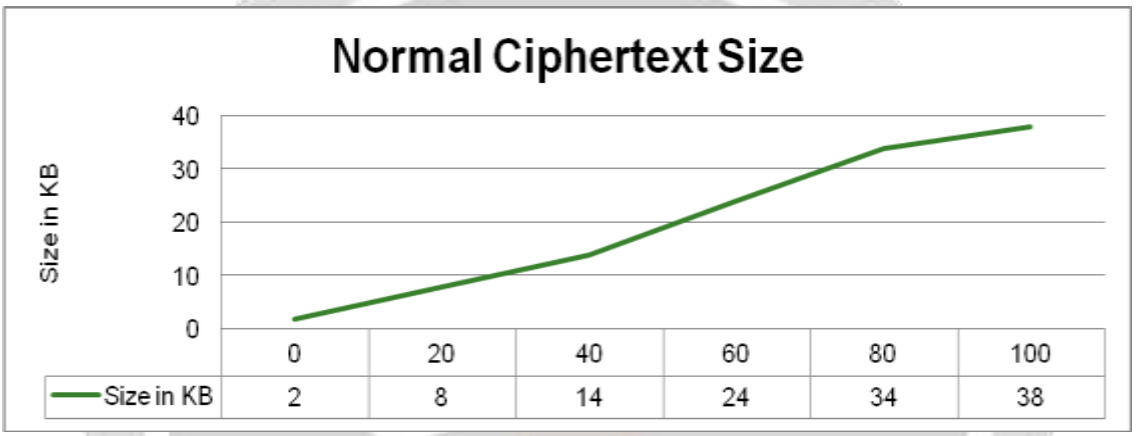


Fig-2- Graph reprsentation of encryption time and upload time in sec.

Data Size in MB	Algorithm Name	Encryption Time in Sec	Upload Time in Sec
10	AES	14	28
100	AES	45	147
200	AES	89	358

Table 1: shows Data Encryption using AES and Cloud Upload

2. Normal cipher text size in different no of policy attribute



7.CONCLUSIONS

In this Paper, the design and implementation detail of proposed system is presented for secure sharing of personal data in cloud computing. To achieve confidentiality and integrity In proposed system proof of ownership has been designed by using hash and tag generation algorithm which will help to implement better security issues in cloud computing environment, also proposed system reduces the computational time to achieve better communication by using attribute based encryption and RCCA standard.

8. REFERENCES

1. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology EUROCRYPT 2005, ser. Lecture Notes in Computer Science, R. Cramer, Ed. Springer Berlin Heidelberg, 2005, vol. 3494, pp. 457–473.
2. Boneh, A. Sahai, and B. Waters, "Functional encryption: Definitions and challenges," in Theory of Cryptography, ser. Lecture Notes in Computer Science, Y. Ishai, Ed. Springer Berlin Heidelberg, 2011, vol. 6597, pp. 253–273.
3. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security, ser. CCS '06. New York, NY, USA: ACM, 2006, pp. 89–98.
4. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proceedings of the 2007 IEEE Symposium on Security and Privacy, ser. SP '07. Washington, DC, USA: IEEE Computer Society, 2007, pp. 321–334.

5. M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of abe ciphertexts," in In: Proceedings of the 20th USENIX Conference on Security, SEC 2011. San Francisco, CA, USA:USENIX Association, Berkeley, 2011.
6. Fujisaki and T. Okamoto, "Secure integration of asymmetricand symmetric encryption schemes," in Advances in Cryptology - CRYPTO '99, ser. Lecture Notes in Computer Science, M. Wiener,Ed. Springer Berlin Heidelberg, 1999, vol. 1666, pp. 537–554.
7. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption," in Proceedings of the 29th Annual international conference on Theory and Applications of Cryptographic Techniques, ser. EUROCRYPT'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 62–91.
8. R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited (preliminary version)," in Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing, ser. STOC '98. New York, NY, USA: ACM, 1998, pp. 209–218.
9. J. Lai, R. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Transactions on Information Forensics and Security, vol. 8, no. 8, pp. 1343–1354, Aug 2013.
10. S. Yamada, N. Attrapadung, G. Hanaoka, and N. Kunihiro, "Generic constructions for chosen-ciphertext secure attribute based encryption," in Public Key Cryptography - PKC 2011, ser. Lecture Notes in Computer Science, D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, Eds. Springer Berlin Heidelberg, 2011, vol. 6571, pp. 71–89.
11. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in Proceedings of the 14th international conference on Practice and theory in public key cryptography conference on Public key cryptography, ser. PKC'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 53–70.
12. T. Okamoto and K. Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption," in Proceedings of the 30th Annual Conference on Advances in Cryptology, ser. CRYPTO'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 191–208.
13. G.Wang, Q. Liu, and J.Wu, "Hierachical attibute-based encryption for fine-grained access control in cloud storage services," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago, IL, 2010.
14. R. Ostrovsky, A. Sahai, and B.Waters, "Attribute-based encryption with non-monotonic access structures," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 195–203.
15. Xianping Mao, Junzuo Lai, Qixiang Mei, Kefei Chen, Jian Weng "Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption" DOI 10.1109/TDSC.2015.2423669, IEEE Transactions on Dependable and Secure Computing.