ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Providing Security, Integrity and Privacy in Attribute Based Encryption

Paruchuru Udaya
M.Tech,
Department of CSE,
Swarna Bharathi College of Engineering, Khammam.

Mr. Mudusu. RamBabu
Associate Professor and HOD,
Department of CSE,
Swarna Bharathi College of Engineering, Khammam.

ABSTRACT:

Cloud computing can be used to enable data sharing capabilities and this can provide an abundant of benefits to the user. The benefits to the organization can gain from data sharing in higher productivity. Data sharing provide efficiency, integrity and privacy of data provider. The high expensive certificate verification in the traditional public key infrastructure is the solution to be efficient. The private key is to specify a particular user. It is not possible when data provider wants to make the private data accessible to designated user key. This problem can solve with a solution is written an agreement delivered to a third party attribute based encryption(ABE) to define a fine grained data access. Cipher text policy attribute based encryption (CPABE) is a method for providing security and data provider can create an encryption format for the data. Decryption is possible only when similar attributes of the user to access.

Keywords:

Multiple Authority CPABE, Security, Data sharing, attribute-based encryption, revocation, access control, removing escrow. Cloud computing, Encryption techniques.

1.Introduction:

Cloud computing has now become a highly demanded service or utility due to the advantages of high computing power, cheap cost of services, high performance, scalability, accessibility as well as availability. Cloud vendors are experiencing growth rates of 50% per annum. But due to being in a stage of infancy, it still has some pitfalls which need to be given proper attention to make cloud computing services more reliable and user friendly.

Cloud computing layers are responsible for different types of services we acquire in figure1.SaaS layer provide access to various software. Iaas manages virtual machines, networks etc. Paas provides facility ford employing a number of applications or services by reducing the high cost and difficulty of buying and governing the primary capabilities of present software and hardware.

Figure 1: Cloud computing layers

2. Related Work:

The user data must be secured by encryption and decryption methods. Data encryption and decryption can done by converting plain text to cipher text using sender's public key. Data decryption can do by converting cipher text to plain text using private key.Key escrow (also known as a "fair" cryptosystem) is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. Removing escrow can be solved by escrow free key protocol. Secure party must be in between KGC (key generation center) and data storing and fine grained policy for each and every attribute by proxy encryption.

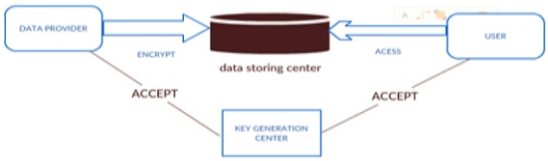
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes (e.g. the country he lives, or the kind of subscription he has). In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. A crucial security aspect of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

3.Literature Survey;

The size of private and public keys must occupy less memory. Public keys is very short user can create cipher text to as many number of users. The private key memory must be low because cryptographic keys will be stored in tamper-resistant memory, which is high in cost. Basically attribute based encryption include key policy attribute based encryption and cipher text policy attribute based encryption. Attribute based encryption which is used to search encryption and also it searches in a hierarchical format.

4. SystemArchitecture:



5. Proposed System:

The security of a two-party computation protocol is usually defined through a comparison with an idealized scenario that is secure by definition. The idealized scenario involves a trusted that collects the input of the two parties over secure channels and returns the result if none of the parties chooses to abort. The cryptographic two-party computation protocol is secure, if it behaves no worse than this ideal protocol, but without the additional trust assumptions. In this paper we propose CP-ABE (cipher text attribute based encryption).it solved a problem of key escrow by dividing authorities for end users private keys. Protective communication by using two party computations between attribute management and key generation, which rectifies secret data of some users. Expect the user no one can acquire the private keys.

Fine grained is a process can done for each and every attribute by proxy encryption format, which is selective group key distribution.

6. System Requirements:

•Works on Windows 7, XP, Vista, 8, 8.1 and 10
•Works on 64 bit Windows
•Mac OS X 10.4 and above

7. Modules:

7.1 Data Provider:

7.1.1 User Login:

User login module contains two fields' username and password. If two fields with correct authorized data then we easily access data. If not it is denied it declares that the user is unauthorized one.

7.1.2 Key Generation:

It is used to grant access permissions for authorized users. Key generation center plays main role on cryptography method. The key may be encrypt or decrypt data as user want to do on data.

7.1.3 Data Provider:

7.1.3.1 Access policy:

Data provider must verify that the user is authorized user all permissions are given to the user. Data provider is responsible for accessing policy before distributing the data.

7.1.3.2 Encryption of file:

Data provider can encrypt a file. Encryption means converting plain text to cipher text which cannot understand easily.

7.1.4 Sending data to data storing center:

Data storing center can store encrypted file and also store user data.

7.2 Data Sharing:

Data storing center is responsible for avoiding the unknown users to share the data and to store the data.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

It provides KGC to authorized key and revokes group of keys to valied users. The services of data storing center are delivering, storage and offsite records.

7.2.1 User Authentication:

If user enter a valued username and password can access data. If not access is completely denied. If the user is new then the user wants to login with username and password. Then the user can access data from data storing center.

7.3 See all Available Files:

It displays all authorized user files and also count the number of files stored in data storing center. The data provider can see all available files for valid users.

7.4 User Receives a File:

User receives a file when access policy is satisfied to encrypt data. The user can select a particular file to decrypt the cipher text from KGC under valid attribute groups.

7.5 Decryption of a File:

Encryption is converting cipher text to plain text and decryption is converting plain text to cipher text. In both encryption and decryption we use cipher text. User can select a particular file can decrypt the file.

8. Implementation:

CP-ABE can implement in data storing center's-ABE uses private keys to user and generates it into master secret keys to set of attributes for user's-ABE consists mainly four parts.

8.1 Setup:

Setup process starts with a security input and returns master private key. the master key is generated by trusted authority.

8.2 Key-Generation Center:

The input from setup process i.e. public key and master key(MK).encryption process includes public key and returns cipher text(CP) that a private key from attributes set S can decrypt the file.

8.3 Decrypt:

Input from cipher text (CT) and returns a message M and satisfies access structure. Attribute set is used to get a master key.

9. Advantages:

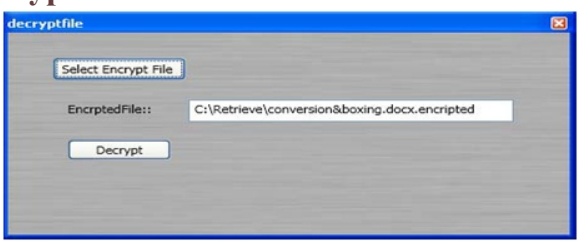
•Secure fine grained access control under sharing.
•Secure 2PC
•Solving escrow key.

10. Snap Shot:

Encryption

File Download

Decryption



11. Future enhancement:

In future it can solve fully distributed approach and also solve many problems like advanced cryptography.

12. Conclusion:

The cipher text policy attribute based encryption is used the technique is used for maintain personal health, records, cloud data storage and in social networks.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The main advantage is increasing security, integrity and efficiency. It also provides security in fine grained data access control in data sharing. The authorized data is secured from outsiders.

References:

[1].S. Yu, C. Wang, K. Ren, W. Lou," Attribute Based Data Sharing with Attribute Revocation," Proc. ASIACCS '10, 2010.

[2].Lewko, A. Sahai, B. Waters," Revocation Systems with Very Small Private Keys," Proc. IEEE Symposium onSecurity and Privacy 2010, pp. 273–285, 2010.

[3].Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. IEEE Symposium on Security and Privacy, 2007 SP'07. 2007; IEEE.

[4]. Liu Q, Wang G, Wu J. Time-based proxy re-encryption scheme for secure data sharing in a cloud environment. Information Sciences. 2014; 258:355–70.

[5].L.Ibraimi, M. Petkovic, S. Nikova, P. Hartel, W. Jonker,"Mediated Cipher text- Policy Attribute-Based Encryption and Its Application", Proc. WISA 2009, LNCS 5932, pp. 309–323, 2009.

[6].Deng H, Wu Q, Qin B, Domingo-Ferrer J, Zhang L, Liu J, et al. Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts. Information Sciences. 2014; 275:370–84.

[7]. Hur J, Koo D, Hwang SO, Kang K. Removing escrow from ciphertext policy attribute-based encryption. Computers and Mathematics with Applications.2013; 65(9):1310–7.