A Survey on Data Security Using File Hierarchy Attribute-Based Encryption in Cloud Computing Environment

A. Banushri, Research Scholar, Department of Computer Science and Engineering, Vels University, Chennai.
E-mail:banushrics.scs@velsuniv.ac.in

Dr.R.A. Karthika, Assistant Professor, Department of Computer Science and Engineering, Vels University, Chennai.
E-mail:karthika.se@velsuniv.ac.in

Abstract--- Cloud computing has formed the conceptual and infrastructural basis for the modern world. Almost all organizations are looking for the ways to decrease the cost and complexity of providing an IT infrastructure. Many organizations frequently deploy cloud based services for every new projector requirements. Privacy and security aspects in a cloud based computing environment remains at the core of interest. Public clouds are managed by the service providers which include servers, storage, networking and datacenter operations. This paper presents a review on the security issues inherent within the context of cloud computing and cloud infrastructure. Ensuring security to the data is an important issue in cloud storage, even though many efforts have been taken to solve the security problem. This paper presents a survey on security issues using Attribute Based Encryption (ABE), Key-Policy ABE (KP-ABE), Cipher-text Policy ABE (CP-ABE) and File Hierarchy Cipher-text policy Attribute-Based Encryption (FH-CP-ABE).ABE uses public-key cryptography by having public key as an arbitrary string. The main concern in this approach is that the decryption can happen only if the user holds the key with matching attributes which are issued by a trusted party. Different from previous cloud based data system, data owners encrypt their secret data for the data receivers using KP-ABE Encryption scheme. Another advanced specification is File Hierarchy Cipher-text policy Attribute-Based Encryption (FH-CP-ABE).In this approach, the data files have the characteristic of multilevel hierarchy. Each layered structures are integrated and then the hierarchical files are encrypted with the integrated access structure.

Keywords--- Access Control, Attribute based Encryption, Key Policy, Cipher-text Policy, File Hierarchy.

I. Introduction

Cloud computing is a model for, on-demand network access and reliable computing resources that can be rapidly provisioned and released with minimal consumer management effort or service provider interaction [1]. Cloud computing evokes different perceptions in different people. To some, it refers to accessing software and storing in the cloud representation of the internet or a network and using associated services. To others, it is seen as nothing new, but a modernization of the time-sharing model.

Cloud computing security threats [16] are:

- Abuse and nefarious use of cloud computing
- Insecure application programming interfaces
- Malicious insiders
- Shared technology vulnerabilities.
- Data loss/leakage
- Account, service & traffic hijacking
- Unknown risk profile

Other security threats are:

- Failures in providers security
- Attacks by other customer
- Availability and reliability issues
- Legal and regulatory issues
- Integrating customer and provider security systems

Solutions to Cloud Security Issues

Many standards have been developed by many groups to provide security to the cloud environment. One such group is Cloud Security Alliance (CSA).CSA gathers solution providers to enter into discussion about the best practices for information security in the cloud. Open Web Application. Security Project (OWASP) is another group which maintains a list of vulnerabilities to cloud based models, which is updated as threat landscape changes. Many extended technologies, concepts are needed that provide secure server which leads to a secure cloud. A layered framework that assures security in cloud computing environment consists of four layers [3].

In Fig. 1, the first layer is a virtual machine layer, in which the concept of virtualization provides a level of freedom of choice for the customer and cost savings for cloud providers. Virtualization also supports utility computing in that a cloud can enable a customer to open virtual machines on the cloud provider's resources as if the virtual instance were running on the customer's hardware. This capability can be extremely useful in meeting a customer's expected and unexpected peak demands. Second layer is a cloud storage layer which integrates resources from multiple cloud service providers. The third layer is the cloud data layer. The fourth layer is the virtual network monitor layer which combines both hardware and software solutions in virtual machines. It handles the problems such as key logger examining [3].

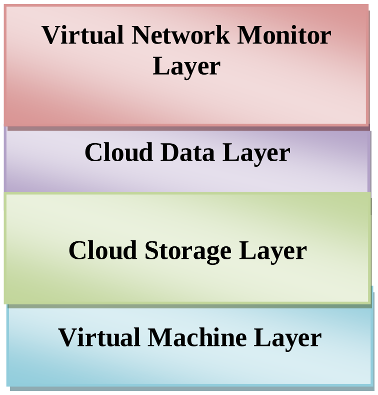

Figure 1: Layered Framework for Cloud Security

Cloud security refers to a broad set of policies deployed to protect data, applications and the associated infrastructure of cloud computing. Security concerns associated with cloud computing fall into two broad categories: security issues faced by cloud providers and security issues faced by their customers [4].The provider must ensure that their infrastructure is secure and that their clients' data and applications are protected, while the user must take measures and use strong passwords and authentication measures. By using some cryptographic algorithms, the data must be encrypted before uploading to the cloud. This approach can provide the confidentiality of the stored data. This paper deals with various categories of attribute based encryption scheme [5][8][11]. Section II deals with literature survey on various encryption algorithms. Section III concludes the discussions of those algorithms.

II. Literature Survey

Before storing the data in the cloud, the users must encrypt the data using efficient encryption techniques. Encryption avoids the unauthorized access of data from the cloud. One of the encryption techniques is Attribute based encryption technique which is used to give the privacy, security and safe access control for the data. Attribute Based Encryption (ABE) Algorithm was introduced to overcome the problem of scalability, flexibility, when the numbers of authorized users increased [5].The Key-Policy ABE (KP-ABE) can achieve more flexibility and also can achieve fine-grained access control than ABE scheme [7].

In KP-ABE, attribute policies are associated with keys and data is associated with attributes. Another modified form of ABE is Cipher text Policy Attribute Based Encryption (CP-ABE) .In CP-ABE, each user is associated with a set of attributes and only authorized users can decrypt by calling the algorithm decryption.

Baodong Qin, Robert H. Deng, Shengli Liu, and Siqi Ma Proposed Attribute-Based Encryption with Outsourced Decryption. In this paper, they presented a scheme to verify the transformed cipher text with outsourced decryption. It works with the key encapsulated mechanism such that ABE cipher text encrypts symmetric session key. Largecipher text size and decryption cost was the drawback of the ABE schemes. The decryption cost grows with the complexity of access policies and the access structures are restricted to AND gates. Later to overcome this problem, an outsourced decryption is suggested [14].

Taeho Jung, Xiang-Yang Li, Zhiguo Wan, and Meng Wan proposed an Access Privilege on cloud data with Anonymous Attribute-Based Encryption. Many techniques have been proposed to control the data access. Identity-based encryption (IBE) was introduced in which the sender can specify an identity and the receiver can decrypt it, if he has matching identity. Few years later, Attribute-Based Encryption (ABE) was suggested which was formerly known as Identity-based encryption (IBE).In this scheme; an identity is viewed as a set of attributes. And decryption is potential if a decryptor's identity overlaps with the specified cipher text. Soon after, tree-based ABE schemes, KP-ABE and CP-ABE were accessible to express more conditions rather than simple overlap [13].

In the KP-ABE, a cipher text is allied with a set of attributes, and a private key is related with an access structure like a tree, which defines the user's identity. A user can decrypt the cipher text if his private key is satisfied by the attributes in the cipher text. The encryptor does not have full control over the encryption policy and he has to trust the key generators. This scheme causes problems in re-encryption [13].On the other hand, this problem is solved in the CP-ABE. In the CP-ABE, cipher texts are generated with an access structure, which indicates the encryption policy, and private keys are created according to users' attributes. A user can decrypt, if his attributes in the private key satisfy the access tree in the cipher text. So the encryptor holds the crucial authority about the encryption policy.

Wenhai Sun, Shucheng Yu, Wenjing Lou, Y.Thomas Hou and Hui Li Proposed Verifiable Attribute-Based Keyword Search. Search over encrypted data is an analytically important technique in cloud computing. Encryption before outsourcing is an essential solution to protect user data privacy. Many secure search techniques have been focused, where the dataset remain encrypted and managed by a single owner, based on symmetric cryptography. This paper presents the attribute-based keyword search scheme with user revocation (ABKS-UR) that enables the fine-grained search authorization. This technique allows multiple owners to encrypt and outsource their data to the server independently [12].

File Hierarchy Cipher-text policy Attribute-Based Encryption (FH-CP-ABE) is the most efficient system compared with all other Attribute-Based Encryption scheme.

Attribute Based Encryption (ABE)

The Attribute Based Encryption (ABE) algorithm was introduced by Sahai and Waters in 2005 to provide security and access control [15]. It is a public-key based encryption that allows users to encrypt and decrypt data based on user attributes. In this Algorithm, the secret key of a user and the cipher text are dependent upon attributes. 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 [2]. The Key Authority produces the keys for the encrypting and decrypting a message based on the user attributes. If the user wants to add some attributes or remove some attributes then the Key Authority will collect the new attributes and generate new public and private key. The message is encrypting using user's public key and receiver will decrypt the message using private key [8][10]. The problem with ABE Algorithm is that, to encrypt data, the data owner's needs to use every authorized user's public key [7].

Key Policy Attribute Based Encryption (KP-ABE)

Another form of ABE is Key Policy Attribute based Encryption and used for one-to-many communication. In this scheme, the encrypted data are connected with set of attributes and secret key are labeled with access tree structure. KP-ABE method gives the efficient result and provides good access control. In cloud server, this scheme helps to lessen the majority of computational transparency overhead [2]. A fine grained access control is provided by the KP-ABE where data is firstly encrypted using the symmetric data encryption key then again re-encrypting that data using public key. The key authority makes decision who can decrypt the data [5]. The problem in this scheme is that the encryptor cannot decide who can decrypt the encrypted data. It is not suitable in some applications because a data owner has to trust the key issuer [9][11].

Cipher- text Policy Attribute Based Encryption (CP-ABE)

CP-ABE is another form of Attribute Based Encryption. Every cipher text is associated with an access policy on attributes and every user's private key is associated with a set of attributes. A user is able to decrypt a cipher text only if the user's private key satisfies the access policy. By using single master key different private keys can be generated using set of attributes. Using access policy, the data is encrypted and the same message is decrypted using asset of attributes [2]. A framework is introduced to know the nature of permission control of encoded information called as Cipher text-Policy Attribute-Based Encryption [9].This technique gives better execution than the other ABE techniques. Utilizing this method, we can keep information more secure in the un-trusted server. This method is closer to the traditional access control methods called as Role-Based Access Control (RBAC).The Data Owner is the main entity in the Architecture of data sharing system, who owns the data and uploads the data into the external data storing center for ease of sharing[15].

Limitations of CP-ABE

The flexibility and efficiency of access control for the enterprise requirements is not completely full filled by these CP-ABE schemes. It has got limitations in specifying the policies and managing the attributes. In this scheme, decryption keys only support user attributes which is organized as a single set. The users can use only all possible combinations of attributes in a single set which is issued in their keys satisfy policies [11]

File Hierarchy Cipher-text Policy Attribute-Based Encryption (FH-CP-ABE)

File Hierarchy Cipher-text policy Attribute-Based Encryption (FH-CP-ABE) is a combination of Hierarchical identity-based encryption scheme (HIBE) and a cipher text-policy attribute-based encryption scheme which was proposed by Wang et al.

An efficient encryption scheme called file hierarchy CP-ABE scheme (FH-CP-ABE) was proposed which is based on layered model of the access structure. FH-CP-ABE extends CP-ABE with a hierarchical structure of access policy. This scheme was proposed to achieve flexible and fine-grained access control [6].This layered access structure is used to solve the problem of multiple hierarchical files sharing where the files encrypted with one access structure. This scheme can resist chosen plaintext attacks (CPA) under the Decisional Bilinear Diffie-Hellman (DBDH) assumption. This scheme has low storage cost and computation complexity in terms of encryption and decryption. This scheme differs from the subsequent CP-ABE schemes. It lightens the burden of key authority center, by distributing the work of key creation on multiple domain authorizations.

The shared files in FH-CP-ABE usually have hierarchical structure. A group of files are separated into a number of hierarchy subgroups situated at different access levels. So the files in the same hierarchical structure might be encrypted by an integrated access structure. This method saves the storage cost of ciphertext and time cost of encryption.

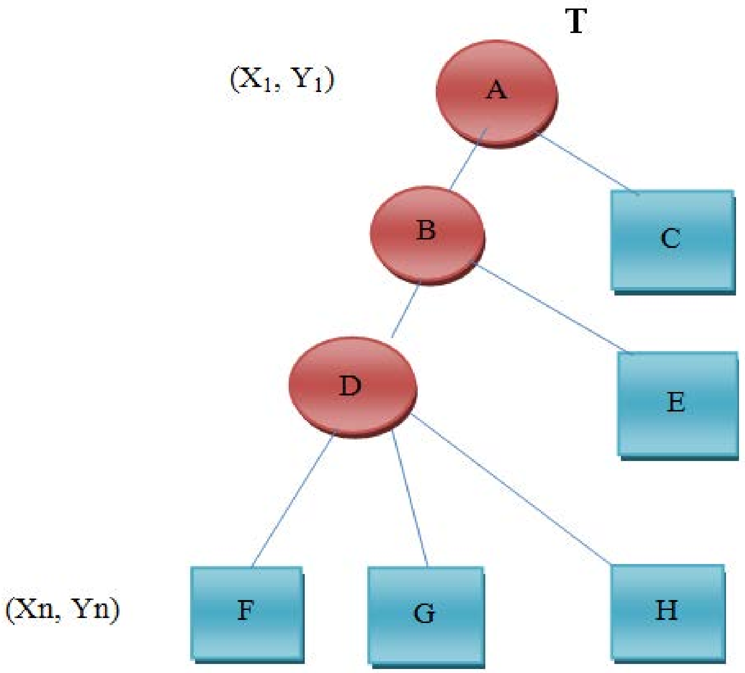

Figure 2: Three-level Access Tree

In Fig.2, T be a hierarchical tree of an access structure divided into n access levels. Circles represent the level node or threshold gate and the square shape represents the attributes. A non-leaf node, denotes a threshold gate such as “AND”,”OR”.

(X_1, Y_I) is the highest hierarchy and (Xn, Yn) is the lowest hierarchy.

This model consists of four different entities such as: authority, CSP (cloud service providers), data owner and user [6]. Assume that the dataowner has n files with n access levels and K= $\{k_1 \ldots k_n\}$ is shared in cloud. Here, K_n is the lowest hierarchy and k1 is the highest hierarchy. If a user can decrypt k_1, the user can also decrypt $k_1 \ldots k_n$.

Authority: In cloud computing, it is a trusted entity and accepts the user enrollment. It executes Setup and KeyGen operations.

Cloud Service Provider (CSP): It is a semi-trusted entity and it can perform the assigned tasks and provides cipher text storage and transmission services.

Data Owner: The data owner has large data to be stored and shared in the cloud. This entity is responsible for defining access structure and executing Encrypt operation and also uploads cipher text to CSP.

User: This entity wants to access a large number of data in cloud environment. The user downloads the corresponding cipher text and executes decrypt operation.

The data owner processes the files in such a way that it first chooses n content keys and encrypts files with the content keys by using encryption algorithm (i.e., DES, AES).And then data owner encrypts using FH-CP-ABE encryption algorithm and obtains a cipher text of content keys.

FH-CP-ABE decryption operation is used to decrypt cipher text and obtains the content key. By using symmetric decryption algorithm with content key, the user can obtain the file.

The FH-CP-ABE Algorithm consists of four operations: Setup, KeyGen, Encrypt and Decrypt.

Setup: It takes the security parameter n as input and outputs public key and master key.

KeyGen: This operation takes public key and master key and a set of attributes and creates secret key.

Encrypt: This operation takes public key, content key and a hierarchical access tree as input and produces integrated cipher text of content keys.

Decrypt: This operation takes public key, cipher text, integrated access structure and a set of attributes as input and if the attributes matches the access structure, then the content keys can be decrypted. Then using symmetric decryption algorithm, the corresponding files will be decrypted with the content keys.

III. Conclusion

In this paper, we analyzed different attribute-based encryption schemes such as ABE, KP-ABE, CP-ABE and FH-CP-ABE. The hierarchical files are encrypted with an integrated access structure and the cipher text related to the attributes. Therefore the cipher text storage and time cost of encryption are saved. The main advantage is that the users can decrypt all authorization files by computing secret key once. If the user needs to decrypt multiple files, the time cost of decryption is also saved. So every method is better than other methods in terms of efficiency.

References

[1] Cloud Computing by Wikipedia, https://en.wikipedia.org/wiki/ Cloud_computing

[2] Lee, C.C., Chung, P.S. and Hwang, M.S. A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments. *IJ Network Security* **15** (4) (2013) 231-240.

[3] Angadi, A.B., Angadi, A.B. and Gull, K.C .Security Issues with Possible Solutions in Cloud Computing-A Survey. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, **2** (2) (2013) 652-661.

[4] Venkata, S., Kumar, K. and Padmapriya, S. A Survey on Cloud Computing Security Threats and Vulnerabilities. *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering* **2** (1) (2014) 622-625.

[5] Ashwini, K.M. and Uma Shankar, B.S. A Review on Attribute Based Encryption (ABE) and ABE Types. *International Journal of Computer Science and Mobile Computing* **5** (5) (2016) 142-146.

[6] Wang, S., Zhou, J., Liu, J.K., Yu, J., Chen, J. and Xie, W. An efficient file hierarchy attribute-based encryption scheme in cloud computing. *IEEE Transactions on Information Forensics and Security* **11** (6) (2016) 1265-1277.

[7] George, M., Gnanadhas, D.C.S. and Saranya, K. A Survey on Attribute Based Encryption Scheme in Cloud Computing. *International Journal of Advanced Research in Computer and Communication Engineering* **2** (11) (2013) 4408-4412.

[8] Lee, C.C., Chung, P.S. and Hwang, M.S. A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments. *IJ Network Security* **15** (4) (2013) 231-240.

[9] Swarup kshatriya and Dr.Sandip M Chaware. A Survey on Data Sharing Using Encryption Technique in Cloud Computing. *International Journal of Computer Science and Information Technologies* **5** (4) (2014) 5351-5354.

[10] Jyothsna, A. and Sandhia, G.K. A Survey on Efficient Security Algorithms In Cloud Computing. *International Journal of Pharmacy & Technology* **8** (4) (2016) 5176-5187.

[11] Nimje, A.R., Gaikwad, V.T. and Datir, H.N. Attribute-Based Encryption Techniques in Cloud Computing Security: An Overview. *International Journal of Computer Trends and Technology* **4** (3) (2013) 419-423.

[12] Sun, W., Yu, S., Lou, W., Hou, Y.T. and Li, H. Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud. *IEEE Transactions on Parallel and Distributed Systems* **27** (4) (2016) 1187-1198.

[13] Jung, T., Li, X.Y., Wan, Z. and Wan, M. Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption. *IEEE Transactions on Information Forensics and Security* **10** (1) (2015) 190-199.

[14] Qin, B., Deng, R.H., Liu, S. and Ma, S. Attribute-based encryption with efficient verifiable outsourced decryption. *IEEE Transactions on Information Forensics and Security* **10** (7) (2015) 1384-1393.

[15] Bethencourt, J., Sahai, A. and Waters, B. Ciphertext-policy attribute-based encryption. *IEEE Symposium on Security and Privacy*, 2007, 321-334.

[16] Kadam, K., Paikrao, R. and Pawar, A. Survey on Cloud Computing Security. *International Journal of Emerging Technology and Advanced Engineering* **3** (12) (2013) 239-249.