© 2017 IJSRSET | Volume 3 | Issue 8 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Enhanced Key Management with Attribute and Access Specification for Data Storage in Cloud Environment

Dr. D. I. George Amalarethinam[*1]**,H. M. Leena**[2]

[*1]Bursar & Director (MCA), Associate Professor, Computer Science Department, Jamal Mohamed College(Autonomous), Tiruchirappalli,Tamil Nadu, India

[2]Assistant Professor , Computer Science Department, Holy Cross College (Autonomous), Tiruchirappalli, Tamil Nadu, India

ABSTRACT

Cloud Computing is an emerging technology with a collection of systems provisioning the resources like hardware, software, processing power, network, operating system, storage on pay-you-go basis. Cloud consumers can deploy these resources from various cloud service providers based on their requirements. Storing the users' sensitive data in cloud is a critical task. Not only securing the data in a proper way is a major concern, but also the access privilege challenges due to the sharing of data stored in cloud is to be considered. The issue of controlling and preventing unauthorized access to data plays a vital role. Thus the access control and permissions on data must be set by the owners of the data based on certain attributes. Hence the proposed system specifies the policy with the given attributes and ensures the access control. This helps in protecting and accessing the data by providing the policy in the key for authenticating and authorizing. The data can be accessed on satisfying the policy and access permissions.

Keywords: Cloud computing, Security, Attributes, Policy, Access Permission.

I. INTRODUCTION

Now-a-days Cloud Computing provides the users, the various abilities to store and manipulate their data in many cloud providers especially public clouds. In turn, the cloud providers or even the third party auditors take all the necessary measures to secure the data of their users. They mainly use the cryptographic methodology for securing the data. Symmetric key algorithms are more preferable than the Asymmetric key algorithms because of its speed. But still the cloud consumers cannot entrust the providers for the possibility of accessing the users' data. Hence the owner of the data began to encrypt their own sensitive data and store that on the cloud. But it is suggested by National Institute of Standards and Technology (NIST) to use symmetric key algorithms which is faster than asymmetric key or any proprietary algorithms. It is also recommended that a major consideration has to be given to key generation and management than data encryption.

To attain the fine grained access control for allowing the users to access the data, Attribute Based Encryption (ABE) was proposed [1] and achieved through public key cryptography. This method encrypts the data based on the specified attributes. The two variations of ABE are Key Policy ABE (KP-ABE) and Cipher text Policy ABE (CP-ABE). In these policy systems, an access tree structure is maintained by the owners over the specified attributes. The intermediate nodes of these trees are threshold gates with which the policy is formed whereas the leaf nodes hold the attributes. In Key Policy Attribute-Based Encryption (KP-ABE) scheme, cipher texts are associated with attribute sets and the private keys are associated with access structures. While in the CP-ABE scheme, attribute sets are associated with the private keys, and cipher texts are associated with access structures. The cipher texts are decrypted only if the access structures are satisfied with the given attributes [2]. KP-ABE scheme is designed for one-to-many communications [3]. In KP-ABE system, user's private key is issued by the trusted attribute authority. The policy in the key decides which cipher texts the key can decrypt. One of the major limitations of KP-ABE is, it can only choose descriptive attributes for the data, and has no choice but to trust the key issuer [3].

II. RELATED WORK

Muhammad Asim et al. [4] presented a new ABE scheme with encryption and decryption outsourcing capabilities. The scheme relies on the use of two semi-trusted proxies, one used to outsource computationally expensive encryption steps and another to outsource decryption steps. During the encryption process, a host involves the encryption proxy to create cryptographic policy components for a set of specified attributes, in such a way that the proxy cannot reveal the original message and is enforced to use the given attributes. During decryption, the decryption proxy is used for policy evaluation.

Jinguang Han et al. [5] proposed a privacy-preserving multi-authority attribute-based encryption (PPDCP-ABE) scheme where both the privacy of the global identifier (GID) and the attributes are concerned. In this scheme, a central authority is not required and multiple authorities can work independently without any cooperation. A user can convince the authorities that the attributes for which he/she is obtaining secret keys are monitored by them without showing the attributes to them.

Jin Sun et al. [6] proposed a key-policy attribute-based broadcast encryption by combining with Waters dual system encryption, attribute-based encryption and broadcast encryption system. Based on the standard model, the scheme can achieve constant-size public parameters, imposes no bound on the size of attribute sets used for encryption and has a large attribute universe. It supports Linear Secret Sharing Scheme (LSSS) matrices as access structures, and provides delegation capabilities to users additionally. The selective security of the proposed scheme is proved by using static, generically secure assumptions in Composite order bilinear groups which do not depend on the number of queries the attacker makes. The analysis results indicated that it has less implementation complexity without increasing of computing efforts.

Guangbo Wang et al. [7] proposed a CP-ABE scheme which can achieve the attribute level user revocation. In this scheme, if some attribute of a user is revoked, then the cipher text corresponding to the revoked attribute is updated so that only the user, whose attributes set satisfies the access control policy and has not been revoked, can carry out the key updating to decrypt the cipher text successfully.

These policy setting algorithms for achieving fine grained access control motivated to set the access control policy in the existing system along with the access permissions.

III. BACKGROUND

Genetic Algorithms provide an optimal solution for most of the optimization problems. Thus, an optimal key is generated by Key Generation Genetic Algorithm (KGGA) [8]. As asymmetric key algorithms like RSA is faster than symmetric algorithms, it can be used for key management rather than data encryption. The generated key is still strengthened by using a proprietary algorithm named Asymmetric Addition Chaining Cryptographic Algorithm (ACCA) [9], a proprietary enhanced RSA algorithm which is faster. This method of encrypting the data by the owners itself paves the way for storing data in the cloud in a more secured way. For data encryption, the three symmetric key algorithms AES, DES, Blowfish are executed and compared with the given encrypted key. Among them Blowfish is faster than other two algorithms. Thus Blowfish algorithm is chosen for data encryption. The data stored in public clouds are geographically distributed. Once the encrypted data is uploaded in the cloud, the owner of the data does not know where the data is actually stored. Some suitable fine grained access control mechanisms and permissions are required to restrict the access of data only to the intended users who are allowed by the owner of the data.

The KGGA algorithm produces a prime optimal key 7757 after the 100th iteration by setting the population size as 10, cross over rate as 0.5 and mutation rate as 0.1. The key generated by the Key Generation Genetic Algorithm (KGGA) is given as input to the Asymmetric Addition Chaining Cryptographic Algorithm (ACCA) for encryption. The aim of this algorithm is to reduce the time taken for encrypting the key by replacing the modular exponentiation of encryption and decryption processes of RSA by the concept of Addition Chaining.

The encrypted Key acts as the key for data encryption using Blowfish algorithm which is faster than other symmetric key algorithms.

IV. PROPOSED SYSTEM

In the proposed system, users are allowed to access the decrypted data in different modes by setting the access policy in the key which is withheld by the owner of the data. The owners of the data can grant the permission to specific users to access their encrypted data in decrypted form based on the attributes like profession, designation, relationship, specialization area etc., The data can still be provided in different modes of access, namely, read, write, or both, according to the attributes. But in the proposed system, the user's key with which they can decrypt the data will not be provided by the key issuer i.e., trusted attribute authority. In turn, the owner of the proposed system, allow the users to access the data based on the policy attached with the key.

According to the proposed system, the policy is set with the specified attributes by the owners of the data for giving the access control to the intended users. The selected users are also given the access permissions based on their attribute values. The file is encrypted and decrypted based on the following algorithms.

Setup: The security parameter is given as the input to this algorithm. The security parameter must be chosen in a way that affects the security aspect of the encryption process. Thus the proposed system uses the key size as the security parameter. The key encrypted by ACCA acts as the public key for encryption used in Blowfish algorithm.

Key Generation: This algorithm inputs the public key and output concatenated key which includes the policy in it.

Encryption: The public key and the plain text are the inputs to the encryption algorithm. It returns the cipher text such that the users whose attributes satisfy the policy can decrypt the data.

Decryption: The inputs of this algorithm are concatenated key and cipher text. The plain text is returned if the policy is satisfied.

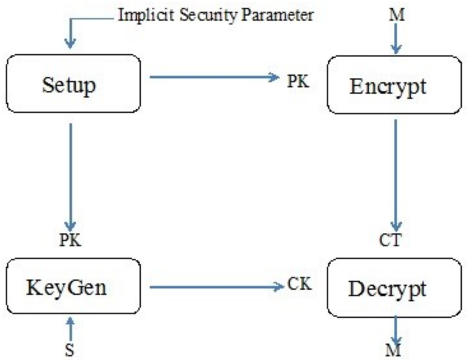

Figure 1. Flowchart of the Proposed System

V. RESULTS AND DISCUSSION

The following example illustrates the proposed system and its working. Designation of the user is chosen as attribute specification. The various classes of designations are Research Scholar, Supervisor, Asst. Professor, and Professor. With the help of these attributes, an access structure and policy is formed with the help of two threshold gates like AND and OR.

Figure 2 shows the Access Tree Structure for the specified attributes.

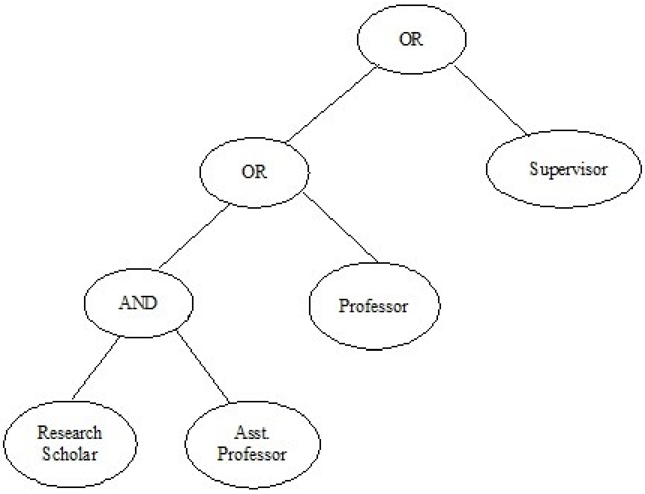

Figure 2. Access Tree Structure

The policy formed with the above access tree structure is ((Research Scholar AND Asst. Professor) OR Professor OR Supervisor)

The policy may differ from one owner to another which can be set for the file stored in the cloud. For example, if the user is an Assistant Professor and also doing his/her Research, then the part of the policy (Research Scholar AND Asst. Professor) is satisfied and the corresponding user will be permitted to view the decrypted file.

In addition to the access control, the user is restricted with the access permissions like read and write or read only on the selected decrypted file. This is achieved by setting the permissions for each of the attributes.

Table 1 shows the comparison of Key-Policy ABE and the proposed system.

Table 1. Comparison Of Kp-Abe And Proposed System

S. No.	**KP-ABE**	**Proposed System**
1	Loses the control since it depends on Trusted Attribute Authority (i.e. Key issuer).	Control is with the owner – No loss of Control.
2	Complexity in deriving the keys of the algorithms.	Less Complex derivation of keys.

VI. CONCLUSION AND FUTURE WORK

The attributes and access control specified in the proposed system enables the restricted access of the decrypted file in the cloud. It shows the secured way of storing the owners' file and giving fine grained access control over the decrypted file. This paves the way for providing authentication and authorization mechanisms to access the decrypted file. In future, this proposed system can be served as a service to the owners of the data in cloud for both secured storage and fine grained access control.

VII. REFERENCES

[1]. Goyal V., Pandey O., Sahai A., Waters B., "Attribute-Based Encryption for Fine-Grained Access Control for Encrypted Data", Proceedings of the 13th Conference on Computerand Communications Security, pp. 89-98, 2006.

[2]. Bethencourt, J., Sahai, A., Waters B., "Ciphertext-Policy Attribute-Based Encryption", Proceedings of the IEEE Symposium on Security and Privacy, pp. 321–334, 2007.

[3]. Parmar Vipul Kumar J, Rajani Kanth Aluvalu, "Key Policy Attribute Based Encryption (KP-ABE): A Review", International Journal of Innovative and Emerging Research in Engineering, Vol. 2, No. 2, pp. 49-52, 2015.

[4]. Muhammad Asim, Milan Petkovic, Tanya Ignatenko, "Attribute-based encryption with encryption and decryption outsourcing", Proceedings of the 12th Australian Information Security Management Conference, pp. 21-28, 2014.

[5]. Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, Man Ho Au, "Improving privacy and security in decentralized ciphertext-policy attribute-based encryption", IEEE Transactions on Information Forensics and Security, Vol. 10, No. 3, pp. 665-678, 2015.

[6]. Jin Sun, Yupu Hu, Leyou Zhang, "A Key-Policy Attribute-Based Broadcast Encryption", The International Arab Journal of Information Technology, Vol. 10, No. 5, pp. 444-453, 2013.

[7]. Guangbo Wang, Jianhua Wang, "Ciphertext-Policy Attribute-Based Encryption with Attribute Level User Revocation in Cloud Storage", Mathematical Problems in Engineering, pp. 1-12, 2017.

[8]. D. I. George Amalarethinam, H. M. Leena, "A New Key Generation Technique Using GA for Enhancing Data Security in Cloud Environment", International Journal of Cloud Computing, 2017.(accepted to be published).

[9]. D. I. George Amalarethinam, H. M. Leena, "Asymmetric Addition Chaining Cryptographic Algorithm (ACCA) for Data Security in Cloud", Springer Verlag, 2017. (accepted to be published).