A Survey on Hierarchical Attribute Set based Encryption (HASBE) Access Control Model for Cloud Computing

Vanraj Kamliya
Research Scholar,
Department of C.E.
School of Engineering,
R.K University, Rajkot

Rajnikanth Aluvalu
Associate Professor
Department of C.E
School of Engineering
R.K University, Rajkot

ABSTRACT

Cloud computing refers to the application and service that run on a distributed system using virtualized resources and access by common internet protocol and networking standard. Cloud computing virtualizes system by pooling and sharing resources. System and resources can be monitored from central infrastructure as needed. It requires high security because of now a days companies going to put more essential and huge amount of data on cloud. That's why the reason traditional access control is not enough For the High security .so that the attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing with the complex access control policy.in this paper, we have proposed hierarchical attribute-set-based encryption (HASBE) access control by extending cipher-text policy and attribute-set-based encryption (ASBE) with a hierarchical structure of users. HASBE provides Flexibility, scalability and fine-grained access control with efficient user revocation but the hierarchical structure of the domain hierarchy is to complex and there is no sub-domain level user hierarchy which increases system response time and decreases the system performance. So we are proposing HASBE scheme by creating a sub domain in to the user level Hierarchy that reduce the complexity of the hierarchy and also improve the system performance.

Keywords

Access Control, Attribute, Cloud computing, Encryption, Decryption, Data Security

1. INTRODUCTION

Cloud computing has rapidly become a widely spread paradigm for delivering services over the internet. Therefore Cloud service provider must provide the trust and security, as there is valuable and sensitive data in large amount stored on the clouds. For protecting the confidentiality of the stored data, one of the way is access control. Access control means the selective restriction of access to a place or other resources. The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization. The traditional access control like ,DAC(discretionary Access control),MAC(Mandatory Access Control),RBAC(Role based access control) and ABAC(Attribute Based Access Control)are not enough for the high security so that various Attribute based Encryption Scheme are proposed.[3] The data must be encrypted before uploading to the cloud by using some cryptographic algorithms [13]. Attribute Based Encryption (ABE) model was proposed by Sahai and Waters [7] in 2005. ABE allows users to encrypt and decrypt data based on user attributes. 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. The problem with attribute based encryption (ABE) scheme is that data owner needs to use every authorized user's public key to encrypt data. So various ABE based access control schemes have been proposed to overcome this problem. Those are Key Policy Attribute Based Encryption (KP-ABE).:KP-ABE was proposed by Goyal et al.[8] in 2006 which is the modified form of classical model of ABE. In KP-ABE cipher text is associated with a set of attributes and user's decryption key is associated with a monotonic tree access structure. Only if the attributes associated with the cipher texts satisfy the tree access structure, can the user decrypt the cipher texts. Cipher text Policy Attribute Based Encryption (CP-ABE):is another modified form of ABE called introduced by Sahai[9]. CP-ABE is used to encrypt the data which can be kept confidential even if the storage server is untrusted [14]. A random number of attributes expressed as strings a primary key is associated. On the other hand, when a data owner encrypts a message he/she specify an associated access structure over attributes. If the data consumer's attributes pass through the cipher-text's access structure then only user can be able to decrypt a cipher text. Hierarchical Attribute Based Encryption (HABE): model was derived by Wang et al [10].it is a combination of (HIBE) and CP-ABE.HABE model has the hierarchical structure consisting of root master at the top, followed by multiple domain masters which consists of set of users and users have the set of attributes.

2. LITERATURE REVIEW

Hierarchical attribute set based encryption (HASBE) which is an extension of HABE (Hierarchical Attribute Based Encryption). In HASBE each data owner/consumer is managed by a domain authority. A domain authority is directed by its parent domain authority or trusted authority. Data owners, Domain authorities, Data consumers, and the trusted authority are prearranged in a hierarchical structure. HASBE uses Bilinear Mapping system for encryption and decryption [12]. Data encryptor specifies an access structure for a cipher text which is referred to as the cipher text policy. Only users with decryption keys whose associated attributes, specified in their key structures, satisfy the access structure can decrypt the cipher text. HASBE uses a recursive set based key structure where each element of the set is either a set or an element corresponding to an attribute.

2.1 System Model

As mentioned in the model Fig.1 we are concerned to implement following main responsibilities: Data Owner, Data Consumer, Domain Authority, and Trusted Authority. User stores data on the cloud which can be retrieved by decrypting the same through a private key provided. This keeps the private data confidential.

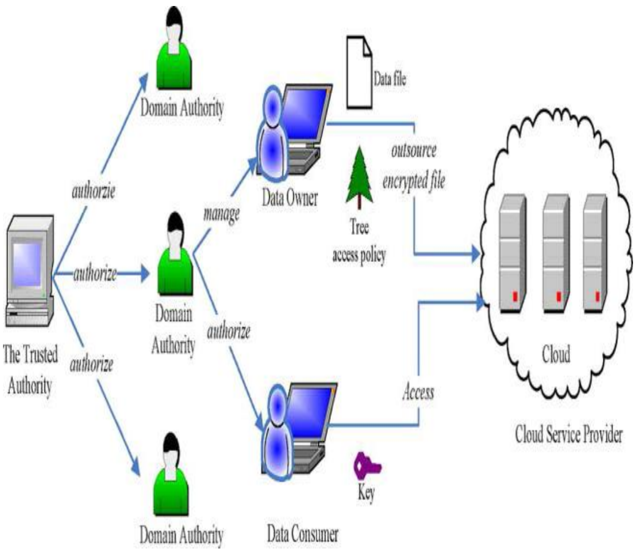

Fig.1.HASBE System Model [1]

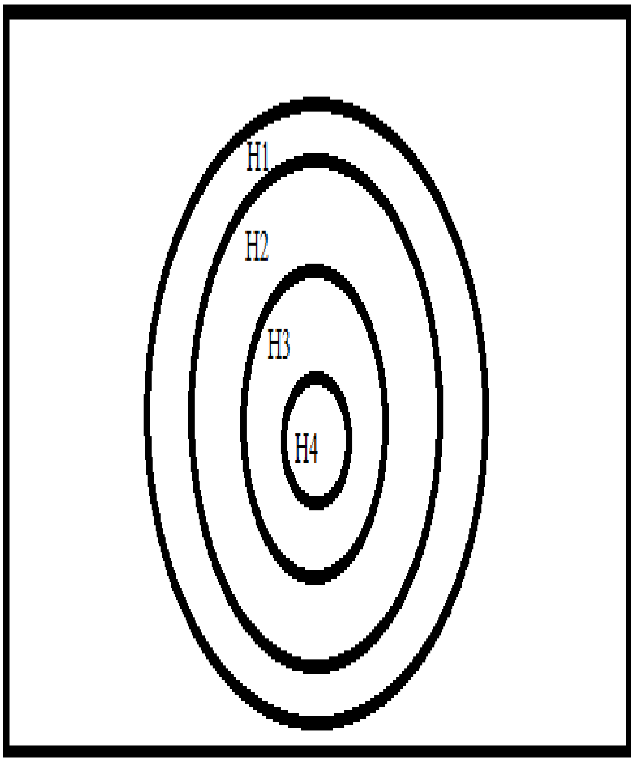

Fig.2.Domain Hierarchy [2]

Here

H = {H1, H2, H3, H4}

Where,

H is cloud

H1 is CEO.

H2 is general manager.

H3 is the list of managers.

H4 is the list of employees.

Firstly, a user has to register with his entire attributes. Once user fills register form then the CEO approves all the details of user, after that CEO provide one key to user. When user gets that key he can access it like a password at the time of login. User will store all data by encryption public key and user can retrieve decrypted data which uses same public key and private key. After that, if user wants to see his own data then he uses the allotted private key and password. When manager wants to access employee’s attribute then master key is used, which is generated by choosing the accessible attributes. If any lower authority is absent then higher authority is responsible for all work related to lower authority. When user is transferred from one location to another location, then all his data is updated in database itself. The manager will assign tasks and guide the employees working under him. Hence the management of assignment of tasks to employees should be done in a manner that is known to himself and respective employee with the permission of CEO in public domain. Also at the time of viewing of his personal information using private domain should be such that he could access it rather than some unauthorized user.

2.2 Key Generation/Encryption/Decryption

The main operations that we need to perform in this section are system setup, data owner grant, data user grant, generating new file, data integrity check, file access, availability check and file deletion.

For security purpose, the proposed scheme consists of 3 keys: Private, Public and Master key. Public key is used in encryption of data, Private and public key is used to decrypt the data and Master key is used for accessing the allowable data.

Setup (d): Here d is the depth of key structure. By taking input a depth parameter d. It gives a public key (PK) and master key (MK).

KeyGen (MK, u, A): By taking the input as master key (MK), user identity and attributes of key structure, it gives private key PRK for user u.

Encrypt (PK, M): By taking the public key (PK), and a message (M), as input. It outputs a cipher-text (CT).

Decrypt (CT, PRK): By taking cipher-text (CT) and private key of user (PRK) as input, it outputs a message (M). If the attributes associated with the user private key (PRK) matches with the access structure of cipher text (CT), then it outputs a message M which is the original correct message. Otherwise, m is null. The modules we consider to perform the above operations are Data Owner Module, Data Consumer Module, Cloud Server Module, Attribute based key generation Module [5]

Bilinear maps: Bilinear maps are the pairing based crypto, it can Establish relationship between cryptographic groups. [6]

The table is the definition of the bilinear map algorithm and the figure-3 shows the working architecture of the bilinear mapping techniques.

Table:1-Bilinear Mapping [6]

Let G1, G2, and Gt be cyclic groups of the same order

Bilinear map from :G1 × G2 to Gt is a function

e: G1 × G2 ⇨Gt

Gt such that for all u belongs to G1, v belongs to G2, and a, b belongs to Z

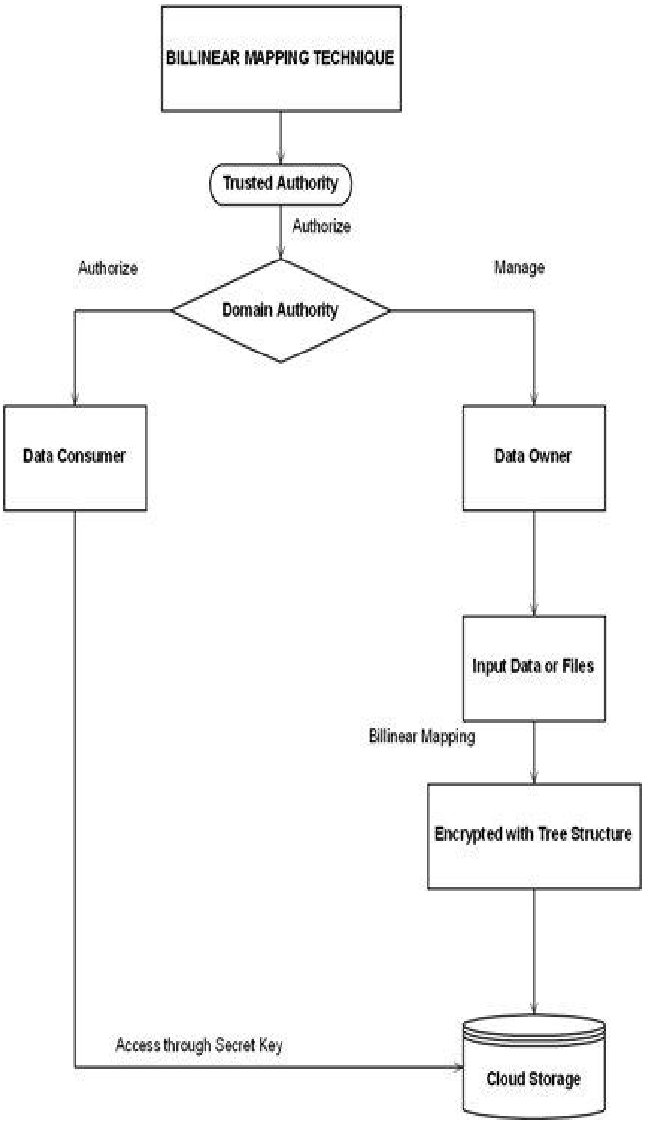

Fig.no.3-Bilinear Mapping [6]

3. PROPOSED SYSTEM

HASBE provides flexibility, Scalability and Fine-grained access control with efficient user revocation .The Domain Hierarchy of the HASBE is very complex and there is no Sub-Domain Level user hierarchy that lead to system was showing complete data related to the requested query even though the employee required some of the data. Due to this, the time to fetch and execute the query was too long. This increased the system response time thereby degrading the system performance. There is also the data was encrypted but the decryption was not restricted to that specific user as keys were not distributed in an efficient way resulting in retrieval of wrong data or incomplete requested data thus increasing chances of hacking. Incase if a lower level authority is absent or is on leave, work is completely stopped and is delayed for the leave duration. Into the proposed system, we enhance Domain Hierarchy by creating Sub-domain for the user that reduces the complexity of the user level hierarchy. Here we are going to create the sub-domain inside the user level hierarchy based on the role of the user.it mean we are going to use role based strategy inside the hierarchy to create the sub-domain that's help at the time of data displaying phase .we can get only required data instead of entire data because of the sub-domain based on role. That's help to improve the system performance as well as decreasing the complexity of the database. For security purpose, the proposed scheme consists of 3 keys: Private, Public and Master key. Public key is used in encryption of data, Private and public key is used to decrypt the data and Master key is used for accessing the allowable data. We are also achieving scalability which manages the workload within company by assigning lower level authority task to higher level authority in case of lower level authority absence or leave. It also involves flexible access of data in which when an employee is transferred to another location/branch, the main database is updated. It reduces the work of manual data transfer.

4. CONCLUSION

Thus, we efficiently provide a Domain level user Hierarchy and fine grained access control with flexibility and scalability with a hierarchical structure in our HASBE system. Our contribution to this paper will be providing security and reduce the complexity of the user level hierarchy by providing sub-domain level hierarchy. And there is also efficiently user revocation it's also efficiently handle the access control when lower level of the authority is absent and update the data periodically when user move to one place to the other place.

5. REFERENCES

[1] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, Senior Member, IEEE ," HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing"in IEEE transection on information forensic and security ., vol. 7, no. 2, April 2012

[2] Sanchal Ramteke, Purva modi, Apurva Raghojiwar, Vijaya Karad, Prof.P.D. Kale.,"HASBE: Hierarchical Attribute based solution for flexible and scalable access control in cloud computing-in International Journal of Scientific and Research Publications, Volume 4, Issue 1, January 2014

[3] Rajanikanth aluvalu,lakshmi Muddana," A Survey on Access Control Models in Cloud Computing"-in Springer International Publishing, Advances in Intelligent Systems and Computing 337, DOI: 10.1007/978-3-319-13728-5_7.

[4] N.krishna. L.Bhavani," HASBE: A Hierarchical Attribute Set Based Encryption For Flexible, Scalable And Fine Grained Access Control In Cloud Computing- International Journal of Computer & Organization Trends –Volume 3 Issue 9 – Oct 2013.

[5] Md.Akram Ali, Ch.Pravallika, P.V.S. Srinivas," Multi-Attribute Based Access Control Policy Enforcement for File Accesses in Cloud"-in International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 5, September 2013

[6] John Bethencourt, Computer Sciences Department Carnegie Mellon University," Intro to Bilinear Maps"

[7] A. Sahai and B. Waters, "Fuzzy identity-based encryption," inProc.EUROCRYPT, 2005, pp. 457473

[8] V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attibute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Alexandria, VA, 2006.

[9] J. Bettencourt, A. Sahai, and B.Waters"Ciphertext-policy attribute based encryption "in Proceedings of IEEE Symposium on Security and Privacy, pp. 321V334, 2007.

[10] Q. Liu, G. Wang, and J. Wu, "Time based proxy re-encryption scheme for secure data sharing in a cloud environment," Information Sciences .In Press, 2012.

[11] S. Gokuldev, 2S.Leelavathi 1Associate Professor, 2PG Scholar Department of Computer Science and Engineering SNS College of Engineering, Coimbatore, India," HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control by Separate Encryption/Decryption in Cloud Computing"-in International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 3, May 2013

[12] Zhibin Zhou and Dijiang Huang Arizona State University On Efficient Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption

[13] Minu George1, Dr. C.Suresh Gnanadhas2, Saranya.K3," A Survey on Attribute Based Encryption Scheme in Cloud Computing"-in International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 11, November 2013

[14] B. Raja Sekhar,B. Sunil Kumar, L. Swathi Reddy, V. PoornaChandar," CP-ABE Based Encryption for Secured Cloud Storage Access"-in International Journal of Scientific & Engineering Research, Volume 3, Issue 9, September-2012

[15] Mauro José A. de Melo, Zair Abdelouahab," A STUDY OF ACCESS CONTROL IN CLOUD COMPUTING ENVIRONMENT" in International Journal of Computers & Technolog Volume 3 No. 3, Nov-Dec, 2012

[16] Punithasurya K, Jeba Priya S," Analysis of Different Access Control Mechanism in Cloud" in International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 4– No.2, September 2012