International Journal on Applications in Electrical and Electronics Engineering
Volume 1: Issue 5: May 2015, pp 7-10. www.aetsjournal.com ISSN (Online) : 2395-3527

Collaborative Multi-Tenant Cloud Computing Based On Multiple Proxies For Secure Network Enforcement

T. Prabu, S. Sivagami

Abstract— Multi tenant data enter is a foundation that backings Internet administration. Cloud computing is quickly changing the substance of the Internet services by empowering even little associations to rapidly construct Web and portable applications for a huge number of clients by exploiting the scale and adaptability of imparted physical frameworks gave by distributed computing. In this situation, various occupants spare their information and applications in imparted servers, smearing the system limits between every inhabitant in the tenant cloud. Furthermore, distinctive inhabitants have diverse security prerequisites, while proxy security in cloud approaches is fundamental to diverse tenant. System virtualization is utilized to meet a differing set of inhabitant particular prerequisites with the basic physical system, empowering multi-occupant data centers to consequently address an extensive and different set of occupant's necessities. In our project synergistic security model framework utilized as a part of a multi-inhabitant server, using VCNSMS with an incorporated collective plan and profound co-operative information with an open source UTM framework. A security level based insurance strategy is proposed for rearranging the security guideline administration for vcnsms. Distinctive security levels have diverse bundle review plans and are authorized with diverse security plugins.

IndexTerm - AccessControl, CloudComputing, Proxy Reencryption, Attribute-based Encryption, Cloud Security.

I. INTRODUCTION

Cloud computing is a term for anything that involves delivering services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service(SaaS).The name cloud computing was stimulated by the cloud symbol that's used to represent the Internet in network diagrams. Cloud as a whole is not a new technology that has emerged, but it has used all other boomed technologies in recent years to provide the best of all services.[12]

Cloud came into reality using a method called Virtualization. Virtualization is nothing but an abstract of the resources that are available.

T. Prabu, PG Scholar, Department of Information Technology , Dhanalakshmi Srinivasan Engineering College, Tamilnadu, India. (Email: prabusaran007@gmail.com)

S. Sivagami, Assistant professor, Department of Information Technology, Dhanalakshmi Srinivasan Engineering College, Tamilnadu, India. (Email:ssivagami186@gmail.com)

The Infrastructure-as-a- Service (IaaS) provider like Amazon Web Services provides virtual server instances with unique IP addresses and provides blocks of storage on demand. Customers use the provider's Application Program Interface (API) to start, stop, access and configure their virtual servers and storage.

Currently the secured data storage mechanism in cloud is still in surfacing stage and it is not very popular across organization and individual users. Primary reasons of low usage are data security and Internet availability. Some of the security issues are very critical and a must be handled in an "AttributeBasedEncryption (ABE)" [1] in this access control system, each cipher text is labeled by the encrypted with a set of descriptive attributes. Each private key is associated with an access structure that specifies which type of cipher texts the key c and encrypt. It only permits an authority to issue private keys that express threshold access policies, in which a certain number of specified attributes need to be present in the cipher-text in order for a user to decrypt.

Access tree structure is used to construct the key. In the tree construction, each non-leaf node represents a threshold gate and leaf node of the tree is described by an attribute and threshold valueas1.Theciphertextsareprovidedwith a set of descriptive attributes. Privatekeys are identified by a tree-access structure in which each interior node of the tree is a threshold gate and the leaves are associated with attributes. A user will be able to decrypt a ciphertext with a given key if and only if there is an assignment of attributes from the ciphertexts to nodes of the tree such that the tree is satisfied. Once the key is obtained, re-randomization is applies over the key using random polynomial. "KeyPolicy-Attribute based encryption (KP-ABE)"[3].This technique was introduced by Goyalet.al.to provide access control in the cloud environment. For the purpose of helping the data owner to enjoy fine-grained access control of data stored on un-trusted cloud servers, a feasible solution is provided by encrypting data through certain cryptographic primitives, and disclosing decryption keys only to authorized users. Un-authorized users, including cloud servers, are not able to decrypt since they do not have the data decryption keys. It uses Decisional bilinear Diffie-Hellman assumption along with the linear secret sharing scheme. It considers the non-monotone attributes for assigning policies. One critical issue in this approach is how to achieve the

desired security goals without introducing a high complexity on key management and data encryption. To

International Journal on Applications in Electrical and Electronics Engineering
Volume 1: Issue 5: May 2015, pp 7-10. www.aetsjournal.com ISSN (Online) : 2395-3527

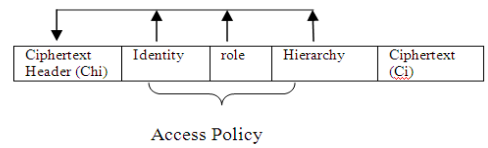
resolve this issue, AccessControlList (ACL) for fine-grained access control is introduced. Several file groups for efficiency. As the system scales, however, the complexity of the ACL-based scheme would be proportional to the number of users in the system. The file group-based scheme, on the other hand, is just able to provide coarse- grained data access control. It actually still remains open to simultaneously achieve the goals of fine-grainedness, scalability, and data confidentiality for data access control in cloud computing.

"Cipher text Policy-Attribute based encryption(CP-ABE)"[4].This technique is proposed by "John Be then court et.al". In this each user is associated with a set of attributes. User secret key is associated with an access structure. Dataare encrypted over a set of attributes. Decryption of data requires the data attributes to satisfy the user access structure. To detect illegal user, their identities IDs should be included in the private key of attribute listL. There is no userID information in the cipher text. This scheme makes use of bilinear map assumptions where the attribute is attached to the private key of the different users. It takes the advantage of owner having the control of distribution of data. It is resistant to multiple collusion attack. "Hierarchical Attribute Set Based Encryption (HASBE)"[10] This HABE is proposed by ZhiguoWanet.al for providing access control. The HABE model consists of a RootMaster(RM) that corresponds to the third trusted party (TTP),multiple do main masters(DMs) in whom the top-level DMs correspond to multiple enterprise users, and numerous users that correspond to all personnel in an enterprise. The RM, whose role closely follows the root Private key Generator, (PKG)

HABE system is responsible for the generation and distribution of system parameters and domain keys. The DM, whose role integrates both the properties of the domain PK Gin a HIBE system and in a CP-ABE system, is responsible for delegating keys to DMs at the next level and distributing keys to users. The left most DM enable the second level to administer all the users in a domain, just as the personnel office administers all personnel in an enterprise, and not to administer any attribute. The other DMs administer an arbitrary number of disjoint attributes, and have full control over the structure and semantics of their attributes. In the HABE model, each DM and attribute is assigned a unique identifier (ID), but marks each user with both an ID and a set of descriptive attributes. Then an entity's secret key is extracted from the DM administering itself, and an entity's public key, which denotes its position in the HABE model, to be an ID tuple consisting of the public key of the DM administering itself and its ID, e.g., the public key of DMi with IDi is in the form of(PKi−1; IDi), the public key of user U with IDu is in the form of(PKu-1; IDu),wherePKi−1,PKu-1are assumed to be the public keys of the DMs that administer DMi, U respectively. This scheme uses cipher text policy based encryption along with the hierarchical identity based encryption. It provides unique identifier to each user along with their descriptive attribute structure.

II. SYSTEM STRUCTURE

The dynamic nature of cloud does not let the existing security schemes to be used as such. The pervious ideas are all focused on smaller and static network. The static network will have predefined set of users and attributes and access structure can be predetermined. In dynamic scenario users may join or leave and group structure will be changing often. The key that has to



Devised for specific user should have validity only till the member remains in the group, otherwise key should get expired. Moreover attributes cannot be defined unique for each user and one-to-one mapping between user and attributes cannot be done. The Hierarchical structure used will have a higher authority whose control of the entire structure. The Domain authority under the higher authority offers key structure to the users and has control of users within the domain and possibly other domains. The users under the domain authority may be either data owner or can be data sharer. The assumption made here is the data sharers are only allowed to have the read access over the file which has shared. The figure1 represents the hierarchical structure of the system used. These interpretation provoked us to propose a new access service mechanism for dynamic cloud computing.

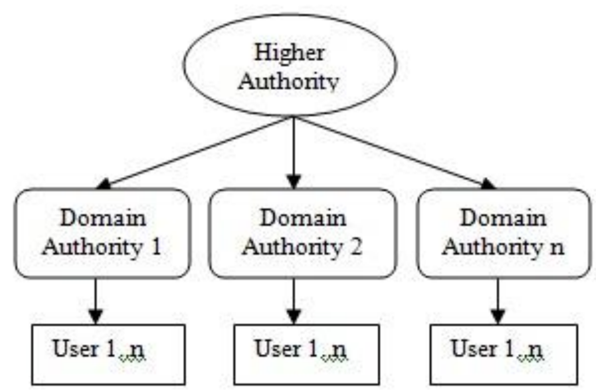


Fig1: System Structure

In this proposed system, it allows any user to have their data secured through encryption amongst each data is shared between different sharers according to the control what they have on data. It uses proxy re-encryption scheme that emphasis security to be given by cloud leveraging the work done by the user. To achieve this, hierarchical identity role based proxy re-encryption scheme is proposed. It allows a user to encrypt his data under his identity to protect this data from leaking and, at the same time, to delegate his data management capability to the cloud.

Furthermore the user could delegate his access control capability to the cloud, which could grant the access of an authorized user under the role heplays, considering his place in his hierarchy, and by transforming the ciphertext encrypted with the data owner's identity to the one with the sharer's identity. The data sharer, who had already registered with data owner, is provided with the secret key. That secret key is used for proxy re-encryption scheme by the cloud. So that the sharers in the future using their secret key generated could decrypt data based on their identity. The different sharer's identity corresponding to different proxy re-encryption key is generated at the time of their registration. When the data owner provides the proxy re-encryption key to the cloud, the cloud can convert the cipher text outsourced by the data owner to the ciphertext that can be decrypted by the sharer. The illustration is given in Table1.In this the data owner uploads the encrypted file to the cloud. Then the cloud performs the Proxy-Re-encryption using the sharer's identity and stores it in the database. Whenever the user wants to access the file he retrieves it by decrypting the file using his secret identity.

Table1: Task Schedule

DataOwner	Cloud	DataSharer
Encryptsdata	Stores Data given by data owner	Registers itself for Authorization with Data Owner
Authorizes Data-sharer	Applies Proxy Re-encryption	Requests data From cloud
Provides secretkey	Sends data to the Sharer	Decrypts the Data using its secretkey

A. SystemSetup

In this phase, important tasks are done. Initially security parameter is taken as input. It helps to design the access tree under which the message is encrypted. It outputs the parameters public and private key (PUa, PRa).Each user in the system is associated with access structure which specifies the attributes associated with the user's decryption key.

B. KeyGeneration

The random algorithm which takes the set of attributes Atti and Private Key PRa as input and outputs the key DKb for decryption based on set of attributes in the list.

C. DataEncryption

The random algorithm which takes Public key, Message M and access Tree as input over the set of attributes. The Ciphe rtext Ci is produced. The cipher text indeed will contain the access structure within it for decryption.

Fig2: FileStructure

$$Ci=(PUa;E(PRa,M) \quad (1)$$

$$Chi=(PUa,AS:(ID,R,H)) \quad (2)$$

The keys for encryption are generated whenever the data owner chooses a file for uploading. The data owner encrypts the data Based on public key parameters and access structure is defined over the cipher text using the cipher text header. After the data being placed in the cloud, the cloud service provider will perform the proxy re-encryption over the encrypted data.

D. Datasharing

In this phase the proxy re-encryption scheme allows the given proxy re-encryption key to translate the ciphertext which is encrypted under PU a into ciphertext of the data sharer under the publickey. Each sharer has to register with the system and obtain a secretkey corresponding to his identity and role in the hierarchy,

$$sk=Hash(ID+role)=HIRBE(IDRu) \quad (3)$$

The secret key is generated as the Hash function of the sharer's identity. There-encryption keys k will be used by the cloud to transform the cipher text Ci to the cipher text under sharer's secret key. The data owner need not be online always so the data owner forwards sk to the cloud which means that the cloud is delegated to manage the data on behalf of the owner. The cloud can deploy there-encrypt key sk to permit the authorized user to get the cipher text decrypted with his own secret key.

E. Data access

The data sharer initially generates the data file request to the cloud server. The cloud server which maintains the secret key on behalf of the data owner wills end the requested data to the data sharer. The data sharer will decrypt the file using the secretkey.

$$Ci=(E(IRBE(IDs),(c(f))=(E(sk,(F.e(PRa)) \quad (4)$$

Then the sharer fetches there-encrypted data from the cloud servers, and runs the Decrypt algorithm on My with his secret key to obtain the

$$D(F)=C(F)=Dec(sk,C) \quad (5)$$

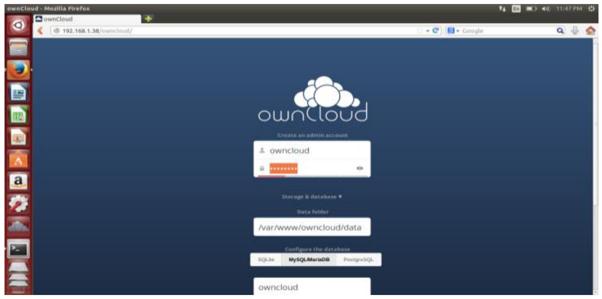
Then for obtaining the original file uploaded by the owner, the user have to perform another ecryption using the owner's public key (PUa).The original file is generated as

$$F=Dec(PUa,D(F)) \quad (6)$$

Any sharer can obtain the required file with the permission of the data owner.

III. RESULT ANALYSIS

Fig 3(a)



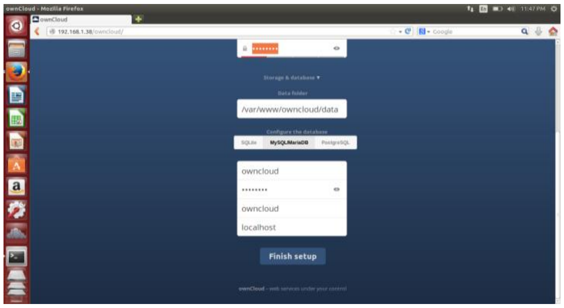


Fig 3(b)

The implementation uses the capable toolkit that use sparing– Based Cryptography library.

The data owner encrypts a file to create a new encrypted file. The time required for the operation

depends on the access tree and key structure. The Number of attributes is assumed to be 30 and the relation between number of attributes and key generation time is compared. Also number of attributes and the decryption time is compared.

Numberof Attributes	Key Generation Time(s)	Authority Grant
10	0.2	2
20	0.4	5
30	0.6	6
40	0.8	9
50	1.0	11

The table2 shows the number of authorization grant given by the higher authority considering different number of attributes for various key generation time. Figure 2 shows the file decryption time considering the number of attributes.

IV. CONCLUSION:

Control of data and also guarantees the data privacy in the cloud the communication and computation cost of the user is highly reduced since the proxy encryption and secret key allocation is pushed to cloud service provider side. The scheme also lets the data owner not to be online always. At the same time, the cost of updating of access policy and communication is also reduced in this mechanism. Each user has an identical key based on their Identity there will be no duplicates. Each user is registered with the Administrator and the user only knows the secret key and owner there will be no unauthorized access. As the data is forwarded to the cloud in encrypted format, it does not have any knowledge about the data. Though the intruders get the data from the cloud they cannot decrypt the data. As the encrypted data as the double wrapping is done over the data and keys are only transferred once that lets the computation cost to be comparatively low. There is no limitation imposed on the number of the data sharer. In this paper, Hierarchical, identity and role attribute based encryption scheme is explored. It offers fine-grained access

REFERENCES

[1] V.Goyal, O. Pandey, A.Sahai, and B. Waters, "Attribute- based encryption for fine-grained access control of encrypted data," in CCS, ACM, 2006, pp.89–98.

[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in INFOCOM 2010, pp.534–5.

[3] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute- based encryption with non-monotonic access structures," in ACM Conference on Computer and Communications Security, 2007, pp.195–203.

[4] Bethencourt J, Sahai A, Waters B."Cipher text- policy AtributeBasedEncryption". In: Proceedings ofISSP; 2007.p. 321-34.

[5] BonehD, FranklinM., "Identity-based encryption from the Weil pairing". In: Proceedings of CRYPTO. LNCS, vol. 2139; 2001. p. 213-29.

[6] Y.Zhu, H.Hu, G.-J. Ahn, D.Huang, and S.Wang, "Towards Temporal Access control in clouds," in Proc.IEEE INFOCOM, pp.2576-2580, 2012.

[7] Yu,C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing," in INFOCOM, IEEE, 2010, pp.534–542.

[8] Y. Zhu, H. Hu, G. J. Ahn, M. Yu, and H. Zhao, "Comparison- based encryption for fine-grained access control in clouds," in CODASPY,ACM,2012.

[9] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in EUROCRYPT, Springer, 2005, pp.457–473.

[10] ZhiguoWan, Jun'eLiu, Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", IEEE Transactions on Information Forensincs and Security, Vol.7, NO.2, April2012.

[11] Tim Mather, Subra Kumaraswamy, shahed Latif, "Cloud Security and privacy: An Enterprise respective of risk and compliance Theory in practice".