ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 5, September 2013

Multi-Attribute Based Access Control Policy Enforcement for File Accesses in Cloud

Md.Akram Ali, Ch.Pravallika, P.V.S. Srinivas
PG Scholar, Assistant Professor, Professor, TKR College of Engineering & Technology
Hyderabad, India

Abstract*—Cloud computing, the imminent need of computing as a finest utility, has the latent to take a enormous leap in the IT industry, is structured and put to optimal use with regard to the current tendency. Keeping in view of high security and privacy concerns, many access control schemes have been proposed. After facing lot of problems from these schemes, a Hierarchical Attribute-Set-Based Encryption [HASBE] scheme came in to existence by providing scalability, flexibility and fine-grained access features. In this paper, we propose Multi-Attribute Based Access Control Policy Enforcement for File Accesses in Cloud. Here, we ensure users to have access privileges to all the data files and re-encrypting the associated data files to make sure that revoked users cannot have any access on those data files. To deal this same concept in cloud, we add an expiration time attribute and a domain authority is required to maintain state information of user keys, which makes our concept in this paper more efficient.

Index terms—**Access Control Schemes, Access Control Policy Enforcement, Bilinear Mapping, expiration-time, User Revocation**,

I. INTRODUCTION

The term cloud computing refers to the delivery of scalable IT resources over the Internet, as opposed to hosting and operating those resources locally, such as on a college or university network. There are four different deployment models of cloud computing. They are Public cloud, Community cloud, Hybrid cloud and Private cloud.

A. Public Cloud: A public cloud, or external cloud, is the most common form of cloud computing, in which services are made available to the general public in a pay-as-you-go manner [10]. The public cloud model is widely accepted and adopted by many enterprises because ,the leading public cloud vendors as Amazon, Microsoft and Google, have equipped their infrastructure with a vast amount of data centres, enabling users to freely scale and shrink their rented resources with low cost and little management burden.

B. Private Cloud: A Private Cloud, or internal cloud, is used when the cloud infrastructure, proprietary network or data centre, is operated solely for a business or organization, and serves customers within the business fire-wall [10].

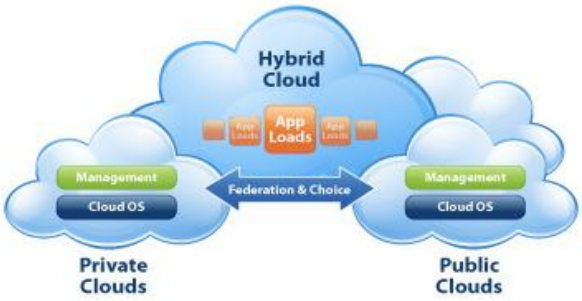

Fig. 1: Deployment Models of Cloud Computing

C. Hybrid Cloud: A composition of the two types (private and public) is called a Hybrid Cloud, where a private cloud is able to maintain high services availability by scaling up their system with externally provisioned resources from a public cloud when there are rapid workload fluctuations or hardware failures [10].

D. Community Cloud: The idea of a Community Cloud is derived from the Grid Computing and Volunteer Computing paradigms. In a community cloud, several enterprises with similar requirement can share their infrastructures, thus increasing their scale while sharing the cost [10].

The benefits of cloud computing for an enterprise include, increased flexibility and market agility as the quick deployment model of cloud computing increases the ability to re-provision rapidly as required.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 5, September 2013

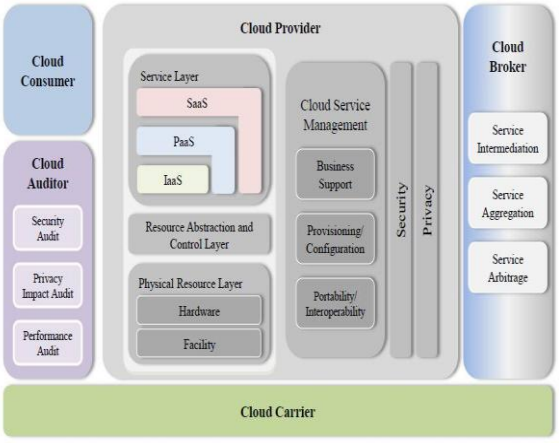

Fig. 2: Architecture of Cloud

II. TYPES OF CLOUD SERVICES

A Cloud is essentially a class of systems that deliver IT resources to remote users as a service. The resources encompass hardware, programming environments and applications. The services provided through cloud systems can be classified into Infrastructure as a service (IaaS), Platform as a Service (PaaS) and Software as a service (SaaS)[9].

A. Infrastructure as a service

The IaaS is categorized into:

1) Computation as a Service (CaaS), in which virtual machine based servers are rented and charged per hour based on the virtual machine capacity – mainly CPU and RAM size, features of the virtual machine, OS and deployed software[9].

2) Data as a Service (DaaS), in which unlimited storage space is used to store the user's data regardless of its type, charged per GB for data size and data transfer.[10]

B. Platform as a service

Platform as a Service (PaaS) cloud systems provide an execution environment that application services can run on. The environment is not just a pre-installed operating system but is also integrated with a programming-language-level platform, which users can be used to develop and build applications for the platform [10][2].

C. Software as a Service

Software-as-a-Service (SaaS) is based on licensing software use on demand, which is already installed and running on a cloud platform. These on-demand applications may have been developed and deployed on the PaaS or IaaS layer of a cloud platform. SaaS replaces traditional software usage with a Subscribe/Rent model, reducing the user's physical equipment deployment and management costs. The SaaS clouds may also allow users to compose existing services to meet their requirements. This section presents some SaaS clouds and applications [10]. Cloud computing encourages IT organizations and providers to increase standardization of protocols and processes so that the many pieces of the cloud computing model can interoperate properly and efficiently. Cloud computing's scalability is another key benefit to higher education, particularly for research projects that require vast amounts of storage or processing capacity for a limited time. Some companies have built data centres near sources of renewable energy, such as wind farms and hydroelectric facilities, and cloud computing affords access to these providers of "green IT."

Access control is the selective restriction of access to a place or other resource. They are the security features that control how users and systems communicate and interact with other systems and resources. Access controls give organization the ability to control, restrict, monitor and protect resource availability, integrity and confidentiality. Keeping in view of all these mandatory things, various access control models have been proposed. The drawback of those access control models is that, the data owners and service providers are not present in the same trusted domain in cloud computing. Later, a new access control scheme was proposed by Yu called as Key-Policy Attribute-Based Encryption (KP-ABE) to enforce fine-grained access control. Due to lack of scalability and flexibility in attribute management, it failed. Cipher text-Policy ABE (CP-ABE) plays a key role to enforce access control of encrypted data [1].

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 5, September 2013

In this paper, we propose Multi-Attribute Based Access Control Policy Enforcement for File Accesses in Cloud. By this, we can achieve scalable, flexible and fine-grained access control with a hierarchical structure of system users by taking help of HASBE scheme in cloud computing. The other sections in the paper include motivation which describes the different schemes that are raised before HASBE. The other section describes our approach towards the proposal and next section is followed by the implementation and evaluation of the proposal work. The final section concludes the paper.

III. ACCESS CONTROL SCHEMES

In this section, we discuss all the different access control schemes which provide a facility like availing of data to the user even during the fault occurrence situation in the cloud. To attain flexibility and fine-grained access control, many access control schemes have been proposed. The main drawback of these schemes is they are applicable to the system in which the data owners and the service providers present within the same trusted domain. Later, to overcome this drawback, a new scheme called as Attribute-Based Encryption [ABE] proposed by Yu[7]. Expressibility lacking is the main drawback of ABE scheme. ABE schemes are classified in to Key-Policy Attribute-Based Encryption [KP-ABE] and Cipher text-Policy Attribute Based Encryption [CP-ABE] based on the association of attributes and access policy with cipher texts and user decryption keys. The main problem with KP-ABE scheme is, here the encryptor is only able to choose descriptive attribute for the data and has no choice other than to trust the key issuer. The drawback with CP-ABE scheme is, the users here can only use all possible combination of attributes that are organized logically as single set. This results in lacking of flexibility and fine-grained access. To overcome all these drawbacks and to achieve scalability, flexibility and fine grained access control; Zhinguo has proposed a Hierarchical Attribute-Set-Based Encryption [HASBE] scheme [1].

IV. PROPOSED ARCHITECTURE

System Architecture:

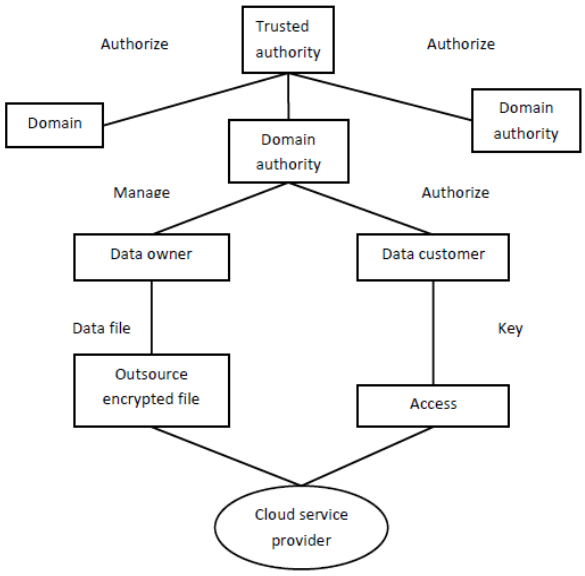

Fig. 3: System Model

From the above figure, the cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. Each data owner/consumer is administrated by a domain authority. A domain authority is managed by its parent domain authority or the trusted authority. Data owners, data consumers, domain authorities, and the trusted authority are organized in a hierarchical manner. The objective of this work is to expand HASBE scheme to realize scalable, supple, and fine-grained access control in cloud computing. The HASBE method flawlessly integrates a hierarchical structure of scheme customers by concerning an allocation algorithm to ASBE. The scope of the project is to build up a new computing technology necessitates users to hand over their precious data to cloud providers, thereby raising safety and confidentiality concerns on outsourced data[4].

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 5, September 2013

In our system, neither data owners nor data consumers will be always online. They come online only when necessary, while the cloud service provider, the trusted authority, and domain authorities are always online. The cloud is assumed to have abundant storage capacity and computation power. In addition, we assume that data consumers can access data files for reading only. In the hierarchical structure of the system users given in Fig. 2, each party is associated with a public key and a private key, with the latter being kept secretly by the party. The trusted authority acts as the root of trust and authorizes the top-level domain authorities. A domain authority is trusted by its subordinate domain authorities or users that it administrates, but may try to get the private keys of users outside its domain[3]. Users may try to access data files either within or outside the scope of their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges. In addition, we assume that communication channels between all parties are secured using standard security protocols, such as SSL.

V. IMPLEMENTATION OF ACCESS CONTROL POLICY ENFORCEMENT

The main operations that we need to perform in this section are system setup, data owner grant, data user grant, generating new file with digital signature, data integrity check, file access, availability check and file deletion. These desirable operations are implemented by using six algorithms, Setup, KeyGen, Message-Digest, Digital Signature, Encrypt, and Decrypt.

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 a secret key SKu for user u.

Message-Digest (M, h): By taking the message M and hash function (h) as input, it gives the message-digest (MD) as output.

Digital-Signature (MK, MD): By taking the message-digest (MD) and master key (MK) as input, it outputs a digital signature.

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

Decrypt (CT, SKu): By taking cipher-text (CT) and secret key of user (SKu) as input, it outputs a message (M). If the attributes associated with the user secret key (SKu) matches with the access structure of ciphertext (CT), then it outputs a message M which is the original correct message[5]. 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.

Bilinear Maps: Let G,G_1 be cyclic (multiplicative) groups of prime order p . Let g be a generator of G. Then e: GXG -> G_1 is a bilinear map if it has the following properties:

• *Bilinearity*: for all u,v Є G and ,a,b Є Z_p, $e(u^a,v^b)=e(u,v)^{ab}$.

• *Nondegeneracy*: $e(g,g) \neq 1$.

G is called a bilinear group if the group operation and the bilinear map e are both efficiently computable.

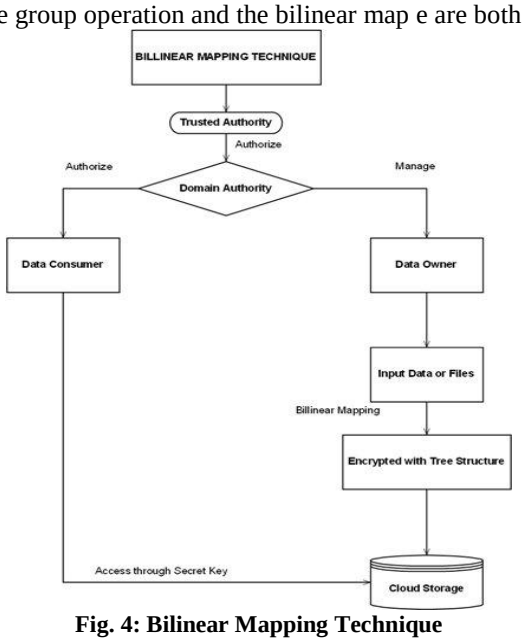

Fig. 4: Bilinear Mapping Technique

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 5, September 2013

A.Domain authority

Domain authority is called as root authority which is responsible for creating the data owner. Domain authority calls the system setup algorithm to generate the public key(PK) and master key(MK), where public key will be made public to other parties and master key will be kept secret. Setup (d=2) → (PK, MK). Here d is the depth of key structure. Here in this paper we consider a key structure of depth 2, and it can be extended to any depth *d*. The algorithm selects a bilinear group G of prime order *p* with generator *g* and then chooses random exponent α, βi ∈ *Zp*, Vi {1, 2}. To support key structure of depth *d*, *i* will range from 1 to *d*. This algorithm sets the public key and master key as follows:

PK= (G, g, h1=$g^{\beta 1}$, f1=g1/β1, h2=gβ2, f2=g1/β2, e (g, g) α)

MK= (β1, β2, gα).

B.Data Owner Module

Data owner is created by the domain authority. Data Owner caries the operation like creating the data user, generating a new file with digital signature, data integrity check and file deletion [6].

1) Creating the Data Users

Data users are created by data owner. At the time of creation, data owner calls the keygen algorithm which gives the secret key for a data user. The secret key is generated by making use of master key and user attributes i.e. key structure of user, where this secret key is sent to the user at the time of creation.

a) Key Structure

Key structure defines unique labels for set in it. The depth of the key structure is the level of recursions in the recursive set which is similar to definition of depth for a tree. Here we consider a key structure with depth 2, members of the set at depth 1 can either be attribute elements or sets. Depth 2 may only be attributes elements. The Fig 4.1 key structure of user represents the attribute of a person who is student in CSE department. The key structure of user and master key is combined to generate the secret key. The Fig 4.2 represents the secret key of user which is the combination of the master key, user id, and user department and user designation.

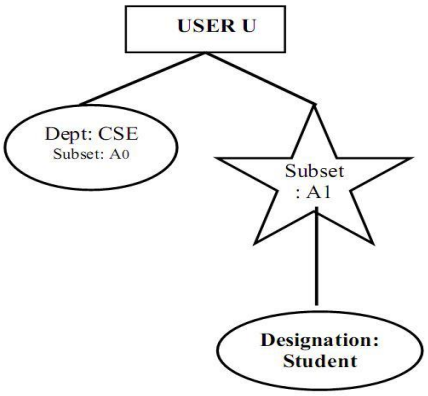

Fig 5: Key structure of user

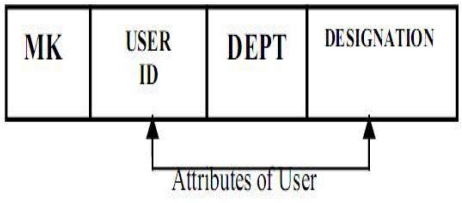

Fig. 6: Secret User

Once the secret key is generated it is sent to the user. The depth of the key structure can be increased by adding the extra attributes. Data owner can add an attribute like expiration-time to user's secret key which indicates the time until which the key is considered to be valid. Once the time expires then the key will be considered as invalid and user will no longer have the file access rights. To perform this key expiration-time operation, access structure associated with data files must include check on expiration-time attribute as a numerical comparison. For e.g.: assuming a user 'U' has a key with expiration-time 'X' and a data file whose access policy is associated with expiration time 'Y', then user 'U' can decrypt the data file only when X>=Y.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 5, September 2013

b) Generating New File with Digital Signature

Once the data owner creates the file, he picks the unique ID for this data file. With the help of hash function the data owner generates the message digest for the corresponding file where further this message digest is encrypted and called as digital signature. This digital signature is appended to file and owner calls the encrypt algorithm which returns cipher-text which is stored in public cloud and redundant copy of that file is saved in a private cloud to achieve a availability. Owner also defines the tree access structure for created files[3].

C.Data User

Data user is created by the owner. At the time of creation, secret key is sent to the user by the data owner. The secret key is the combination of master key and user attributes like user id, user department and user designation.

1) File Access

If there is a need for user to download the file, then user must send the request by specifying the file name or file id with secret key to the gateway server. Gateway server accepts the request and extracts the attribute value present in the secret key of user. Gateway server sends the request for access details to access control tree by specifying file name and attributes. Once the access details of specified file is obtained by access control tree, then server matches the access structure of file with user attributes. If attributes and access structure matches then gateway server sends the request to the cloud storage and picks the requested file and calls the decrypt(CT, SKu) algorithm which decrypts the cipher-text and sends the decrypted file to the user, if match is not found, then user access rights to the requested file is denied.

2) File Availability

Availability can be achieved by using the hybrid cloud concept where the redundant copy of the file will be saved in the private cloud. Even though the file which is requested by the user has not found in public cloud due to its deletion by cloud service provider, user will get the requested file with the use of hybrid cloud concept. Initially gateway server will send the request for the public cloud by specifying requested file id, if the particular file has not found in the public cloud then gateway server will send the request to private cloud where the redundant copy is stored and picks the particular file from the private cloud, decrypts it and sends the file to user [5].

D.Cloud Server Module

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.

E.Attribute based key generation Module

The trusted authority is responsible for generating and distributing system parameters and root master keys as well as authorizing the top-level domain authorities. A domain authority is responsible for delegating keys to subordinate domain authorities at the next level or users in its domain. Each user in the system is assigned a key structure which specifies the attributes associated with the user's decryption key. The trusted authority calls the algorithm to create system public parameters PK and master key MK. PK will be made public to other parties and MK will be kept secret. When a user sends request for data files stored on the cloud, the cloud sends the corresponding cipher texts to the user. The user decrypts them by first calling decrypt (CT, SK) to obtain DEK and then decrypt data files using DEK[9].

(*)User Revocation: Whenever there is a user to be revoked, the system must make sure the revoked user cannot access the associated data files any more. One way to solve this problem is to re-encrypt all the associated data files used to be accessed by the revoked user, but we must also ensure that the other users who still have access privileges to these data files can access them correctly [8].

VI. EMPIRICAL EVALUATION : ANALYSIS AND REPORTS

With the control, a field authority DA can carry out New User/Domain Authority Grant for a new user or one more domain authority in his domain. The charge depends on the number of subsets and attributes to be entrusted. Suppose the domain authority DA has a private key with some number of attributes. When DA wants to delegate some amount of the attributes, the cost produces linearly with the number of subsets to be assigned. This has been implemented by a HASBE scheme based on the CP-ABE which uses the Pairing-Based Cryptography [8].

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 5, September 2013

Fig. 7: Domain Authority Registration

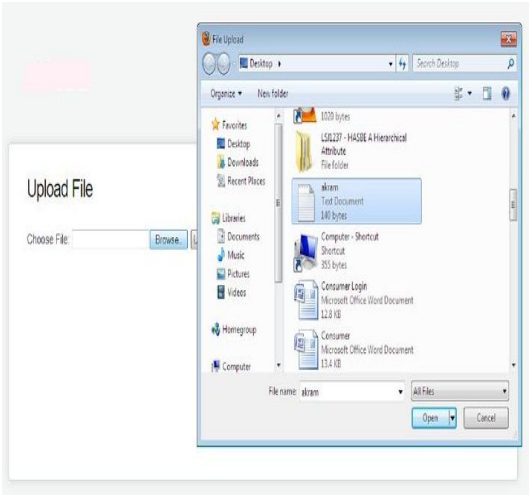

Fig. 8: To upload a file

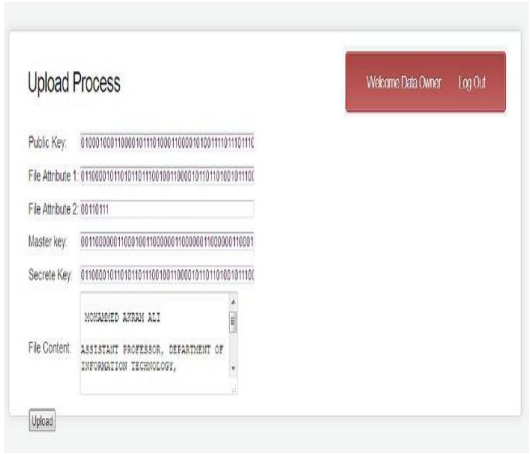

Fig. 9: Upload process

The time taken to generate the secret key with number of attributes in key structure in new user grant operation is given below.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 5, September 2013

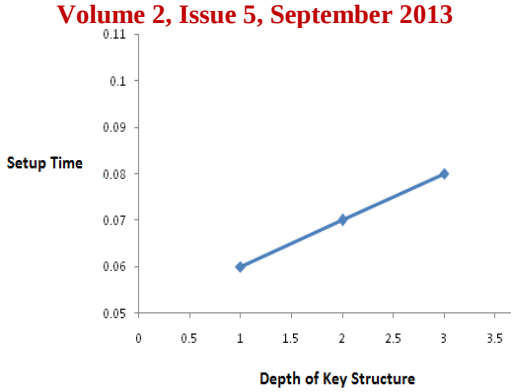

Fig. 10: Setup operation

Fig.10 shows the time required to setup the system for a different depth of key structure. Our scheme can be extended to support any depth of key structure. Setup can be completed in constant time for a given depth.

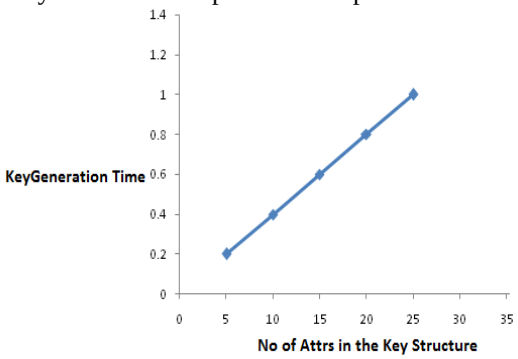

Fig. 11: New user grant

Fig.11 shows the time required to generate the key considering number of attributes in the key structure.

VII. CONCLUSION

The HASBE scheme seamlessly incorporates a hierarchical structure of system users by applying a delegation algorithm to ASBE. HASBE not only supports compound attributes due to flexible attribute set combinations but also achieves efficient user revocation because of multiple value assignments of attributes. In this paper we formally proven the better way to achieve multi-attribute based access control policy enforcement for file accesses in cloud. As HASBE inherits the advantage of ASBE in efficient user revocation, by excluding the revoked users, the other users can have access privileges to the data files.

REFERENCES

[1] HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing Zhiguo Wan, Jun'e Liu, and Robert H. Deng

[2] IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.

[3] R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Comput. Syst., vol. 25, pp. 599–616, 2009.

[4] P. D. McDaniel and A. Prakash, "Methods and limitations of security policy reconciliation," in Proc. IEEE Symp. Security and Privacy, Berkeley, CA, 2002.

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

[6] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute based encryption," in Proc. IEEE Symp. Security and Privacy, Oakland, CA, 2007.

[7] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Proc. ESORICS, Saint Malo, France, 2009.

[8] A. Sahai and B. Waters, "Fuzzy identity based encryption," in Proc. Advances in Cryptology Euro crypt, 2005, vol. 3494, LNCS, pp. 457–473.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 5, September 2013

[9] G.Wang, Q. Liu, and J.Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago, IL, 2010.

[10] R. Martin, "IBM brings cloud computing to earth with massive new data centers," InformationWeek Aug. 2008 [Online]. Available: http://www.informationweek.com/news/hardware/data_centers/209901523.

[11] "Deploying an Application on the Cloud" N. Ram Ganga Charan, S. Tirupati Rao, Dr. P.V.S. Srinivas in (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 5, 2011.

AUTHOR BIOGRAPHY

MD. Akram Ali, B.Tech Graduate in Computer Science and Engineering from Vaagdevi College of Engineering and Technology. He is pursuing Masters from TKR college of Engineering & Technology. Attended workshops on trends in Cloud Computing, Ethical Hacking. He worked in research under the guidance of Prof. Dr. P.V.S. Srinivas on Multi-Attribute Based Access Control Policy Enforcement for File Accesses in Cloud.

CH. Pravallika, presently serving as an Assistant Professor in the Department of Computer Science and Engineering at TKR College of Engineering & Technology. She has got Masters from CVSR college of Engineering. She worked as an Assistant Professor in various colleges for more than 3 years in the Department of Computer Science and Engineering.

Dr. P.V.S.Srinivas is presently serving as a Professor & Head, Department of Computer Science and Engineering, at TKR College of Engineering and Technology, Hyderabad. He has got his Masters followed by PhD in Computer Science and Engineering in the area of Computer Networks from JNTU Hyderabad in the year 2003 and 2009 respectively. His main research interests are Wireless Communication, Mobile Computing and Mobile Ad hoc Networks. His research focus is on "Designing an Effective and Assured Communication in MANETs" and improving QoS in MANETs. He has a rich experience of total 20 years, out of which 2 years of Industry and 18 years of academic. He is also serving as a Chief Panel Consultant in the area of wireless communications for a Hyderabad based company by name SCADA METER SOLUTIONS Pvt Ltd. He has published 46 research papers in different refereed International journals and conferences in India as well as Abroad. He is also serving as an Editor-in-Chief for an International Journal IJWNC and also a peer reviewer for 3 International Journals.