Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DYNAMIC STRUCTURED PRIVILEGES WITH MULTI-OWNER DATA SHARING FOR DYNAMIC GROUPS IN THE CLOUD

[1]A.VELAYUDHAM, [2]M.M RAMYA SELVI, [3]B.HARIHARAN, [4]G.V.S GOHILA

[1]Assistant Professor (SG), Department of IT, Cape Institute of Technology, Levengipuram – 627114, India
PG Scholar, ME (Computer and Communication), Cape Institute of Technology
[3]Assistant Professor, Department of IT, Cape Institute of Technology, Levengipuram – 627114, India
[4]PG Scholar, ME (Computer and Communication), Cape Institute of Technology
E-mail: [1]a.velayudham@gmail.com, [2]ramyasmm91@gmail.com, [3]hariharanb31@yahoo.com, [4]gohila.gvs@hotmail.com

ABSTRACT

Cloud Computing is a general term used to describe a new class of network based computing that takes place over the Internet. The most basic and important service offered by cloud is data storage. However the major obstacle in the multi owner data sharing for the wide deployment of cloud computing is identity privacy while preserving data. In the existing approaches, a secure multiowner data sharing scheme, named Mona is used, for dynamic groups in the cloud that uses the group signature and dynamic broadcast encryption techniques. But this method to invoke and revoke of client is not dynamic on user privileges. Also the system supports only static groups. In the proposed scheme, we present an efficient structure for facts and figures sharing scheme to achieve dynamic privileges. Using this structure, any data owner can change the service class of each user dynamically and change the structure of privileges flexibly when it is needed. The proposed is also designed to support group migration between the users so that the users can revocate and change the group at any time. Thus by using the dynamic structure privileges, the system performs linearly with the increase in the number of users. But in the existing approaches, when the number of users increases the time execution is also increased which makes the system time consuming.

Keywords: *Cloud Computing, Multi Owner Data Sharing, Group Signature, Broadcast Encryption, Dynamic Privileges*

1. INTRODUCTION

Cloud Computing is a technology that makes use of the internet and central remote servers to provide a storage area to the users to maintain data and applications which also which reduces the storage overhead of the users in their devices. Cloud computing allows users to gain the benefits of the applications without installation and access their personal files at any computer with internet access. The cloud services offered can be classified in to three categories: Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS) as referred in Figure 1. SaaS is a model of software deployment where an application is hosted as a service provided to customers across the internet. It is becoming an increasingly prevalent delivery model as underlying technologies that support Web services and service-oriented architecture (SOA) mature and new developmental approaches, such as Ajax. Meanwhile, broadband service has become increasingly available to support user access from more areas around the world. Platform as a Service (PaaS) is a service where the customers with the assistance of internet access will rent hardware utilities, operating systems, storage resources and network capacity. Also with the help of this service delivery model the customers are able to rent the virtualized servers and associated services for running existing applications or developing and testing new ones. The different applications for platform as a service are Google App Engine, Joyant, and Salesforce etc. Infrastructure as a Service is a provision model in which a company outsources the equipment used to support operations, including storage, hardware components, servers and networks. This is useful for the small organization where the cost of spending too much amount in hardware and other components can be minimized. The service provider owns the equipment and takes the responsibility for maintaining it and provides services to the users with the help of brokers. The

Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

client typically pays on a per-use basis. It is provided by the cloud service providers (CSP's) such as amazon, GoGrid etc.

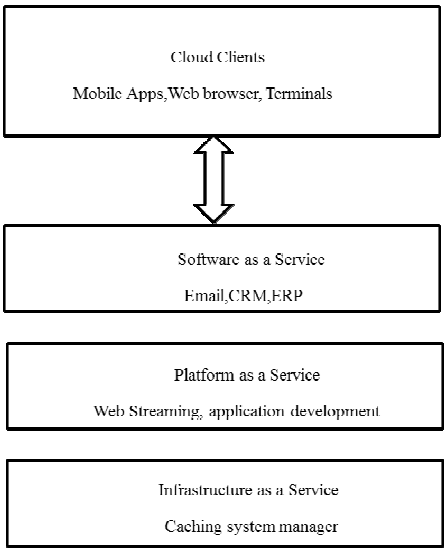

Figure.1 Cloud Services

Cloud computing offers three types of deployment model in which the cloud users are offered the pay-as you go basis in the public cloud. Various service providers such as amazon, Microsoft and google own the infrastructure and offer access to the requested users via the internet. In the private cloud, the infrastructure is owned by a single organization which is managed internally or externally by a third party. The composition of both the public and private cloud makes the hybrid cloud that offers the benefits of the other benefit model. Identity privacy is the one of the major obstacles in the deployment of cloud computing. Without the guarantee of the identity privacy the users may be unwilling to join the untrusted server in the cloud. Another major challenge issue in cloud computing is the availability and maintenance of data. The cloud users must be able to enjoy the data from the cloud this is defined as the multiple owner manner as in [11]. Even though multi-owner data sharing concept is involved in [11] this model does not provide the privileges to the users in the cloud.

The major contributions of our proposed system are that it supports dynamic groups efficiently. It also provides a multi-owner data sharing method so that the scalability of the system is increased. Defining certain privileges to the group members in the cloud reduces the overhead for the group manager.

2. RELATED WORKS

The major challenge issue with the cloud computing is that the network is dynamic and the new users join the cloud on demand.

Goyal et al.[1] and Shucheng et al[4] a new cryptosystem for fine grained system is introduced. Both systems provide a well-defined fine grained access policy. This system defines the enforcing of the access policies based on the data attributes [4]. In the system [1] is named as key policy attribute based encryption. In this approach, the cipher text is decrypted using the private keys. Data is stored on the server in encrypted form.

Sabrina et al. [12] proposed a system with write privileges over outsourced data. Here encryption is based on symmetric keys. Liu et al. [11] a multi owner data sharing method is proposed but this system does not support for dynamic groups. The system supports only static groups [4, 9, 11]. The System also uses group signature where each users sign their messages without revealing their identity [11]. Here broadcast encryption method is used to support static groups.

John et al. [5] proposed a scheme called NetODESSA, an inference-based system for network configuration and dynamic policy enforcement.

Boneh et al. [6] proposed the identity based encryption scheme which simplified the certificate management in email systems. Here both the sender and the receiver have to contact a trusted third party for their key exchange purpose named as the private key generator (PKG).

Dan et al. [9] introduced a system which provides Hierarchical Identity Based Encryption (HIBE). In this system, the ciphertext consists of just three group elements and decryption requires only two bilinear map computations, regardless of the hierarchy depth.

Kallahalla et al. [2] proposed a secure file sharing on the file server which is not a trust system can be enabled by using the cryptographic storage named as plutus. To provide the security and to protect files the system makes use of novel based cryptographic primitives.

Sabrina et al. [7] designed a system with a selective encryption approach to the support of write privileges. The system enriches the approach based on key derivation of existing solutions and complements it with a hash based approach for supporting write privileges. Also the data owner is allowed to verify the integrity of the outsourced data.

Cecile et al. [10] proposed a system with New efficient constructions for public-key

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

broadcast encryption here the receivers are stateless and the encryption is collusion-secure for arbitrarily large collusions of users and security is tight in the standard model; new users can join dynamically i.e. without modification of user decryption keys nor ciphertext size and little or no alteration of the encryption key.

Pratiba et al. [8] a threshold multi signature scheme is introduced. Third party auditor performs the cloud storage auditing. Provides data outsourcing thus the user can be relieved from the burden of data storage security and maintenance. Group signature methods are used [14] and all the group members should sign the messages without revealing the identity of the users.

Ateniese et al. [3] a new re encryption is introduced to increase the security and thus provides a secure file sharing system. Since this system is unidirectional it does not require delegators to reveal all of the secret keys to anyone. Mykletun et al. [13] proposed a system to ensure data integrity and authentication. Here a novel based scheme is introduced which is generated by a single signer.

3. DYNAMIC STRUCTURED PRIVILIGES FRAMEWORK

Cloud is operated by CSPs that offers abundant storage services to the users and for business purposes. However, the cloud is not fully trusted by users since the CSPs are provided by the third party servers who operate outside of the cloud users' trusted domain. As the group manager [11] takes charge of system parameters generation, user registration, user revocation, and revealing the real identity of a dispute data owner. Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group. In the previous methods as [11] the system is not dynamic and the third party is responsible for the data sharing. But in these approaches, data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Since the unauthorized users have no knowledge of the decryption keys, the unauthorized users cannot learn the content of the data.

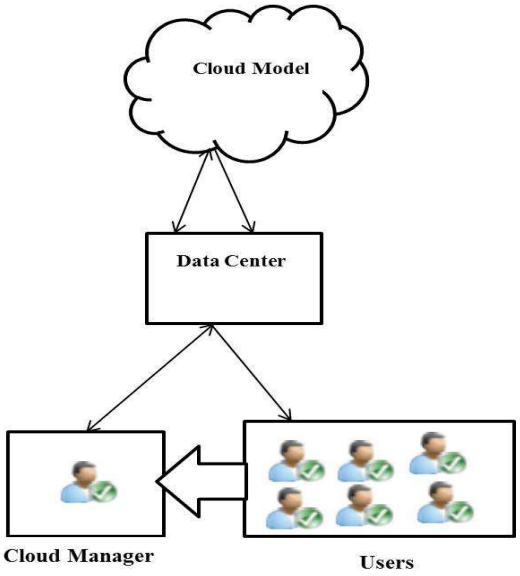

Figure.2 Existing System Model of MONA

Figure 2 presents the system model for MONA where the group manager is responsible for the sharing of data in to the cloud. Also this system does not support dynamic groups. This system is not designed for the data to travel in the reverse direction i.e. the user cannot update any data of their group manager in their group. However in the proposed system we have overcome this problem by supporting the dynamic groups efficiently. Here if a user has to access a data from their higher authorized member in the group then the user has to create their own group. With the new group the user gets the privilege to access the group manager of its previous group and this new group is temporary and after accessing, the data from the group manager the user will return to his own group. Thus the user may not be directly able to contact his/her group manager. But have the privileges to access the data in the cloud. Thus scalability is maintained. And since here we use both private and public keys security is highly provided. Also in this scheme the data user can change the privileges dynamically according to the data sharing and access control as discussed earlier. Thus this system increases the flexibility to change the structure of the privileges when necessary.

Based on any data sharing scheme without considering dynamic privileges, our proposed system can achieve O(T) sets of original ciphertext headers and ciphertext bodies, where T is the number of access groups. We consider the dynamically structured privileged (DSP) as (DSP.Setup, DSP.KeyGen, DSP.GroupInit,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DSP.Enc, DSP.Dec, DSP.AddUser, DSP.RemoveUser, DSP.AddGroup, and DSP.RemoveGroup).This proposed frame work achieves dynamic tree-structured privileges, while previous schemes allow only dynamic line-structured privileges or static privileges as [11, 4, 9]. In this scheme we use different algorithms to achieve the dynamic privileges. The various algorithms are described below.

3.1 DSP.Setup:

DSP.Setup is the algorithm that is used for system setup. By running (PK, SK) DS.Setup (), the data owner obtains PK as the public parameters and SK as private keys for the system. With this algorithm the users create the parameters to access the system and the data owners provide the security of the system using the private key parameters. Finally the users can access the data owner's data with the help of the public key parameters.

3.2 DSP.KeyGen:

DSP.KeyGen is the algorithm that creates the public and private key to the users. By running the DS (SK, u) the users can decrypt the already encrypted messages. Thus by knowing the secret key the users are able to decrypt the data. Thus with the help of the key generation algorithm the users are able communicate in a secure channel.

3.3 DSP.GroupInit:

DSP.GroupInit algorithm is used for initializing the access group of all users in the system. If a user is allowed access the data in a group then his/her identity is put in the group set. Thus the group contains the list of the accessed users with their identity.

3.4 DSP.AddUser:

DSP.AddUser algorithm is used to handle the event when a new user is added to gain access in a certain group. As already discussed when a new user wants to join a group he/she places their identity in the group set and the group manager checks the identity and provide the access control to the user. And the new access policy is updated to the other users informing about the invocation of the new user.

3.4 DSP.RemoveUser:

DSP.RemoveUser is the algorithm which is used to handle the event that some user u is removed from certain access group Gi. Consider that a user u is renewed from the system using the algorithm DSP.RemoveUser. As per our system the user is removed from a group G_i to G_j to the new group G_j to provide certain privileges. The user joins the new group G_j with the DSP.AddUser algorithm.

When user u is removed from G_i all the temporary session keys should be renewed and updated in the group. A new random value is generated to provide the new temporary key in the new group for the user u. Once the work has been completed user u releases from the group G_j using the algorithm DSP.RemoveUser and join its own group. After the user is removed from the group the random values will no longer exist.

3.5 DSP.AddGroup:

DSP.AddGroup algorithm is used to add a new group by the data owner. As mentioned earlier, a user can create a new group to gain the access control of their higher authority for instance. This group can also add different users with the DSP.AddUser algorithm and the identity of all the users are stored in the group set.

3.6 DSP.RemoveGroup:

DSP.RemoveGroup algorithm is used to handle the event when the data owner wants to remove a certain access group. This algorithm is similar to the DSP.RemoveUser algorithm. Removing the group means removing a set of users and their random values are no longer needed.

3.7 DSP.Encr:

DSP.Encr algorithm is used for secure data sharing among the users. The system uses RSA algorithm for encryption purpose. Digital signatures are also used. RSA is a public key crypto system in which the encryption key is public and the decryption key is private. The sender sends the public key to the receiver who keeps the private key secret for decryption and sends the file to the sender along with the key. Referred from the system the encryption and decryption are done [15]. The ciphertext is calculated by using the formula

$$c \equiv m^e (mod\ n) \quad (1)$$

As in system [1] the encryption is done with a set of attributes where the decryption is done only when the attributes are matched. Thus the fine grained access control achieved. Here we use the same method for better encryption with the RSA algorithm.

3.8 DSP.Decr:

DSP.Decr algorithm is used for secure data sharing among the users same as encryption. Here the key is private The sender send the public key to the receiver who keeps the private key secret for decryption and sends the file to the sender along

Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

with the key. The plaintext is calculated by using the formula

$$p \equiv c^d (mod n) \quad (2)$$

Initially the system starts with the user and group registration. According to the privileges given to the users the users may be splitted in to groups. After the creation of the group a random number is chosen and the group manager is chosen. The group manager is responsible for the privilege processing for the users. The data owner is the user interested to share their own data to the cloud or to the group manager. The users will be given read/write privileges. But the user cannot be given the full rights to access the privileges to their group manager due to security concern. The users will have the possibility to read the files but cannot be given permission to update the data within the group. So the user has to form a temporary group with usual process and has to revoke from the previous group. The group manager updates the revocation list and unique number of the user has been removed. The user joins the new group after the registration. The user then transfers the file from the new group with the public key. The group manager who has received a message from the user checks the authenticity of the user and the revocation list. Once the authenticity is verified the user is allowed to transfer the files with the group manager. After completing all the file transfers and updates the user can leave the group and the user can join the previous to which he/she belongs to. The user even though had a membership of the same group previously the user has to again perform the registration with the group manager to ensure security and to avoid unnecessary entries.

4. SYSTEM DESIGN

The proposed system provides an efficient facts and figures scheme to achieve the dynamic structured privileges.

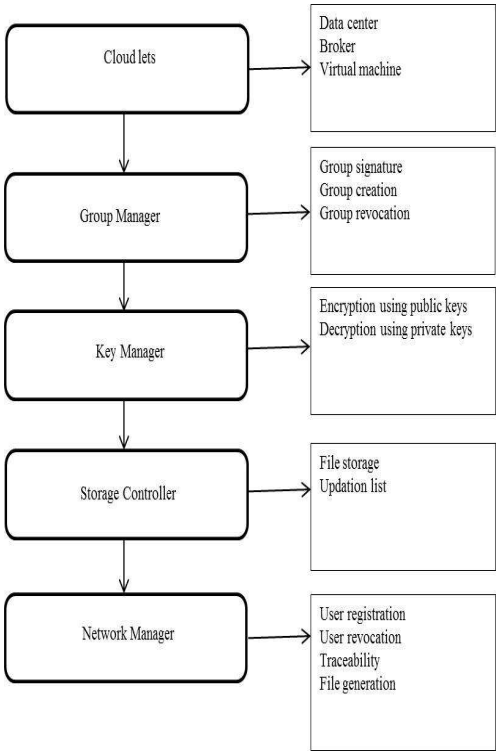

Figure.3 Process Flow Diagram for the Proposed Methodology

4.1 Cloudlet:

The cloudlet is a new architectural element that arises from the convergence of mobile computing and cloud computing. The cloud let has the following sub modules that are data center, broker, and virtual machine. Data center is viewed as the clouds for the file storage.

4.1.1 Data center:

Data center acts a cloud for the group and provides storage space to the users as per their need. The data centers are available to the users any time based on their authenticity given by the group manager.

4.1.2 Broker:

A broker is third party service provider between the cloud service provider and the user.

4.1.3 Virtual machines:

Virtual machine is a software based system that does not exist physically used for resource sharing among the virtual components. Storage in virtual machines reduces the storage overhead space in the personal computers.

4.2 Group manager:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A group manager is responsible for employing group strategy to validate the user within the group for communication. The group manager creates the group and the group manager will maintain the lists of users. The group manager also has the responsibility to maintain the revocation when a user moves from a group.

4.2.1. Group creation:

Initially the users of the same privileges join the group and select a random number to choose the group manager. The group creation is based on the users with the same privileges.

4.2.2 Group signature:

After the group has created group signature has to be done to provide security. All the users in the group sign the messages without revealing the identity of the user this is done as referred in [14]. This group signature will be traceable only to the group manager. When a user wants to revocate from the group his/her identity is selectively disabled from the group without affecting the membership of the unrevoked users. Thus the system is protected from the access of third party members.

4.2.3Group revocation:

Group revocation is the removal of the group. If the group has users with no task then the group can be deleted providing the space for the other groups.

4.3 Key Manager:

A key manager is responsible for employing public and private key pairs to validate your identity when you log into VMs using SSH. Here the keys are assigned and accessed among the primary users .Session is maintained along with the revocation list to provide effective communication among the system.

4.3.1 Encryption using public keys:

As already discussed, the encryptions of the messages are performed using RSA algorithm. Here the sender uses the public key and the receiver uses the private key. Session keys are also maintained.

4.3.2 Decryption using private keys:

The encrypted messages or files received by a user or group manager have to decrypt the original message by checking the authenticity of the sender. Once the authentication was verified, the decryption is done as usual using the private keys.

4.4 Storage manager:

The storage controller is responsible for the Storage information and other data storage related information. Here the controls are assigned and accessed among the primary users and revocation list are maintained to provide effective communication among the system.

4.4.1 File Storage:

Every user has to provide their file to store in the cloud which has to be updated periodically. With the multi-ownership policy this can be achieved efficiently.

4.4.2 Updation list:

The list of users and the number of groups should be maintained as information and should be stored as a file in the file storage. The group manager should maintain this list. And only the group manager can access the updates within this file.

4.5 Network Manager:

The network manager maintains the network based information to validate the cloud network and allow authentication among the system for communication. This network based information includes IP and associated IP based information for cloudlet Processing.

4.5.1 User registration:

The user who has to join the group has to register with the group whose identity is kept secret and traceable only to the group manager.

4.5.2User revocation:

As previously discussed, a user temporarily joins a new group to share file to their higher authorized member. After the task has been completed the user revocate from the group and the revocation list should be updated by the group manager.

4.5.3 Traceability:

The network manager to ensure security among the users performs this. The identity of the users should not be traceable to the third party or the revoked members.

Our system starts with the system initialization. After the initialization, the cloud groups are created. The cloud manager uses the cloud after the cloud data server has been initialized. Once the cloud manager has registered the id with the cloud he has the direct access to the cloud. However our system allows the users also to share data with the cloud only after the group registration so that untrusted member cannot interfere during the files exchange. The registered

Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

users in the have the group share a group key using which they can share the data with the clouds and also can share the data amongst them. Once the user has finished with the sharing he will be revoked from the group and this revocation list will be maintained by the group manager. In our system the sharing of the cloud resources has been shown. Here new user groups can be created dynamically and the multi owner data sharing is also achieved efficiently with increased scalability and flexibility. Once the user has been removed from the group the revocation information should be updated in the group and the new user who joins the group has the knowledge to decrypt the already encrypted messages by the other users.

5. PERFORMANCE ANALYSIS

Generally cloud computing provides a large amount of resources for data storage. With the available cloud services and the internet access users are able to share the resources, hardware and operating systems etc.

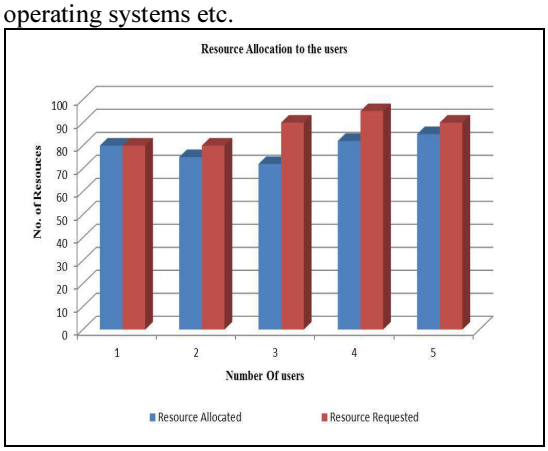

Figure 4: Resource Management

In our system the resource management to the data owners and the users are maintained by the third party service providers of the cloud. When a user is registered with his id to the data owner he will be provided with a certain amount of resources by the brokers according to their demand. Also the unused resource of any user can be taken later for reuse to the other users. Thus our system shows a better resource management. Refer figure 5 that shows the sample for the resource allocation to the users.

In our system the group manager uses the private keys for the encryption and decryption of the messages. The users make use of the public key of the group manager to decrypt the message of the group manager. The group manager stores the master private key and additionally the user list and the shared data list. Thus the group manager uses the more storage resources than the other. The group member's responsibility is to store their private key and their own data. Thus the storage overhead to the users will be reduced strongly.

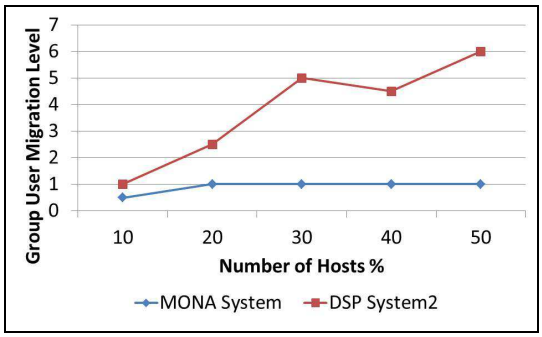

Figure 5: Group Migration Level

The proposed suppotrs dynamic group migration as already discussed. Figure 5 refers to a sample group migration of the users. The existing approach MONA[11] supports dynamic users bt it is not flexible enough to support dynamic operations which is provided in the present system by providing access privileges to the users. In contrast the proposed DSP supports dynamic operations efficiently.

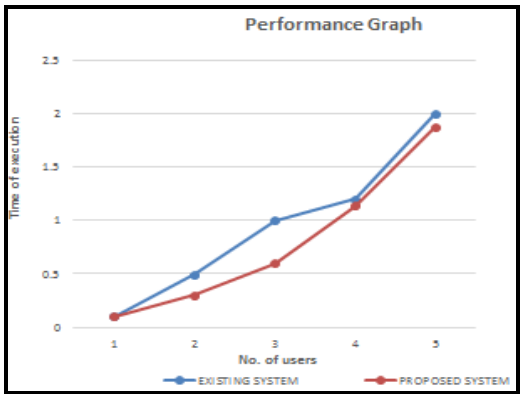

Figure 6: Performance Evaluation Graph

Since the system supports dynamic groups efficiently the performance increases with the increase in the number of the users than the previous methods. The performance result shows that the time of execution increases linearly with the increase in the number of users refer figure 6. In the proposed system we use a dynamic tree structured privileges to achieve the scalability and the dynamicity between the users. Also this system increases the security since the group members are not directly given access to their group managers

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and the users can create the new group dynamically in this system that increases the flexibility. The graph shows that the proposed has a better performance than the previous methods. In the previous method as referred in [11] only the multi ownership between the clouds is provided but the system is not flexible to provide the privileges to the users. The system supports only static groups. So the time of execution is increased will be increased if more number of users are added. Thus performance may be linearly decreased with more number of users. Since the proposed method supports privileges it is more flexible than previous method and the performance is increased linearly. In the system we have shown the results with 5000 hosts and achieved that the resource allocation has been successfully processed.

6. SIMULATION RESULTS

Table 1 specifies the simulation results of the system and have shown the results using the cloudsim. Here we have used 5000 clouds to perform the result. Initially the virtual machine has been set up and the broker initiated. The simulation shows the resource allocation to the users in the cloud. We have considered 5000 hosts and 10 users to show the results. From the simulation, we prove that the time taken by the users to complete the task is the same as the time allocated for them and independent to the number of users. The simulation results mainly focus about the resource allocation to the users.

The simulation results mainly focus about the resource allocation to the users. After the task completed and the cloudlets are executed the simulation destructs the VM and broker. The brokers are destroyed after the work completed so that they do not share the information to the other third party users. After destroying all the virtual machines all the data centers are closed. And the new data centers are created for the other users.

Table 1: Simulation Results

Cloudlet	Status	Data center ID	VM ID	Time	Start Time	Finish Time
0	SUCCESS	2	9	3.7	0	3.7
1	SUCCESS	2	19	3.7	0	3.7
2	SUCCESS	2	29	3.7	0	3.7
3	SUCCESS	2	39	3.7	0	3.7
4	SUCCESS	2	8	4.33	0	4.33
5	SUCCESS	2	18	4.33	0	4.33
6	SUCCESS	2	28	4.33	0	4.33
7	SUCCESS	2	38	4.33	0	4.33
8	SUCCESS	2	7	5.12	0	5.12
9	SUCCESS	2	17	5.12	0	5.12
10	SUCCESS	2	27	5.12	0	5.12

Thus the group is revocated after the task has been completed by destroying the VM and then the data center will be closed. As shown in the fig5 the resource allocated to the users has been shown in the simulation results. Once the data center has been initiated the user who has registered with the group can have access to the cloud. The users not registered with the group can enter the cloud but cannot access the groups. The groups are shared with a private key, provided with more security within the cloud, and given separate space as shown in the simulation results.

7. CONCLUSION

In this paper, we design a multi owner data ownership provided with the dynamic privileges. This system supports dynamic users and dynamic groups efficiently. User invocation and revocation is updated by the group manager so that any changes in the system is reflected to all the users thus the system works more efficiently in all aspects. Here the storage overhead and the performance costs are constant and increase linearly. Our proposed system also satisfies other security issues efficiently. All the existing approaches discussed previously provides only data file sharing with their group manager in this system we propose a dynamic privileged system with multi ownership which increases the flexibility of the system to the users. Also the system supports group migration of the users efficiently. Here we have shown simulation results for the resource allocation of the users. The results also show that the increase in the number of users does not affect the system performance but in the previous approaches, time of execution is increased when the users increase thus degrades the system performance.

REFERENCES

[1] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS) , 2006,pp. 89-98.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[2] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, 2003, pp. 29-42.

[3] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," ACM Transactions on Information and System Security(TISSEC), Vol.9, Issue. 1, 2006, pp.1-31.

[4] S. Yu, C. Wang, K. Ren, and W.Lou,"Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, 2010, pp. 534-542.

[5] John Bellessa1, Evan Kroske, Reza Farivar, MirkoMontanari, Kevin Larson and Roy H. Campbell,"NetODESSA: Dynamic Policy Enforcement in Cloud Networks" 30th IEEE Symposium on Reliable Distributed Systems Workshops(SRDSW), 2011, pp. 57-61.

[6] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), 2001, pp. 213-229.

[7] Sabrina De Capitani di Vimercatia, Sara Forestia, Sushil Jajodiab, Giovanni Livragaa, Stefan Paraboschic, Pierangela Samaratia, "Enforcing Dynamic Write Privileges in Data Outsourcing" 27th IFIP International Information Security Conference, Vol. 39, 2013, pp. 47-63.

[8] D.Pratiba, Dr.G.Shobha, "Privacy preserving public auditing for data storage security in cloud computing", Proc. IEEE INFOCOM , 2010, pp. 1-9.

[9] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2005, pp. 440-456.

[10] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ci-phertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, 2007, pp. 39-59.

[11] Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, Vol.24, no.6, 2013, pp.1182-1191.

[12] S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, P. Samarati, "Support for write privileges on outsourced data," Springer, IFIP Advances in Information and Communication Technology, Vol. 376, 2012, pp. 199-210.

[13] E. Mykletun, M. Narasimha, and G. Tsudik, "Authentication and integrity in outsourced databases," ACM Transactions on Storage, Springer, Vol.2 Issue.2, 2006, pp. 107–138.

[14] D. Boneh, X. Boyen, and H. Shacham. "Short group signatures". Proc. 24th Annual International Cryptology Conference Advances in Cryptology, Vol. 3152, 2004, pp.41-55.

[15] Parsi Kalpana, Sudha Singaraju , "Data Security in cloud computing using RSA algorithm," IJRCCT, Vol. 1 Issue. 4,2012, pp. 143-146.