www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 4 April, 2013 Page No. 986 -990

Implementation of Secret Delegation for Secured Attribute Based Access Control In Cloud Computing

Mrs.G.Mariammal [1] ***Dr.N.Uma Maheswari*** [2] ***Dr.R.Venkatesh*** [3] ***Mr.P.Lakshmanan*** [4]

1. Lecturer, Department of CSE, PSNA College of Engineering and Technology Dindigul, India marisl_g1985@yahoo.com
2. Professor, Department of CSE, PSNA College of Engineering and Technology Dindigul, India numamahi@gmail.com
3. Professor, Department of IT, PSNA College of Engineering and Technology Dindigul, India rlvenkatesh@gmail.com
4. Assistant Professor, Department of Mechanical, RVS College of Engineering and Technology Dindigul,India mars_laksh@yahoo.com

***Abstract*— Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks towards the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper, a new cryptosystem for fine-grained sharing of encrypted data named Cipher text-Policy attribute-based encryption (CP-ABE). The cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. Attribute-based encryption (ABE) has been envisioned as a promising cryptographic primitive for realizing secure and flexible access control. The property based encryption extends the Attribute Set Based Encryption (ASBE) algorithm with a hierarchical structure to improve scalability and flexibility while at the same time it inherits the feature of fine-grained access control of ASBE. At the same time the data integrity of cloud storage is ensured by using (Message-Digest Algorithm) MD5 and Reed Solomon algorithm.**

***Index Terms*— Cipher text-Policy Attribute-Based Encryption, Attribute-based encryption, Attribute set based encryption, Message-Digest Algorithm.**

I. INTRODUCTION

Cloud computing is the delivery of computing as a service rather than a product, whereby we shared resources, software, and information are provided to computers and other devices as a utility over a network. Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. The ever cheaper and more powerful processors, together with the software as a service (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale. The increasing network bandwidth and reliable flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centers. Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management. Cloud computing eliminate the responsibility of local machines for data maintenance. Although the cloud infrastructures are much more powerful and reliable than personal computing devices have a broad range of both internal and external threats for data integrity still exist. In many situations, when a user encrypts sensitive data, it is important that the user can establish a specific access control policy on who can decrypt this data. But for cloud it is a great challenge to provide proper access control to access the data and the other main issue is to ensure the correctness of user's outsourcing data [2]. In order to address this issue the proposed system, we use a new type of encryption method that is a serial property based encryption using attribute based encryption, which provide secure access control and data integrity of system

RELATED WORK

A..Challenges in cloud security

1) *Data protection*: To be considered protected, data from one customer must be properly segregated from that of another; it must be stored securely when "at rest" and it must be able to move securely from one location to another. Cloud providers have systems to prevent data leaks or access by third parties. [6]Proper separation of duties should ensure that auditing and/or monitoring cannot be defeated, even by privileged users at the cloud provider.
2) *Access Control and Accounting:* Heterogeneity and diversity of services, as well as the domains' diverse access requirements in cloud computing environment demand fine-grained access control policies. In particular access control services should be flexible enough to capture dynamic, context or attribute-based or credential-based access requirements and to enforce the principle of least privilege [6].
3) *Identity management*: Every enterprise will have its own identity management system to control access to

information and computing resources. Cloud providers either integrate the customer's identity management system into their own infrastructure, using federation or SSO technology, or provide an identity management solution of their own [6].

4) *Secure-Service Management*: In cloud computing environments, cloud service providers and service

5)

6) *Physical and personnel security:* Providers ensure that physical machines are adequately secure and that access to these machines as well as all relevant customer data is not only restricted but that access is documented[2].

7) *Availability:* Cloud providers assure customers that they will have regular and predictable access to their data and applications.

8) *Application security:* Cloud providers ensure that applications available as a service via the cloud are secure by implementing testing and acceptance procedures for outsourced or packaged application code [2]. It also requires application security measures (application-level firewalls) be in place in the production environment

A. Attribute Base Encryption Techniques

1) Identity based encryption (IBE): For Identity based encryption, we need a trusted third party, but it eliminates the need to do the certificate look up. The idea is as follows: There is a (trusted third party) TTP called KGS (Key Generation Server). Given an identity, KGS generates a private key and the identity acts as the public key. If there is a huge trust placed on the KGS, The security of the whole system relies on the security of the KGS and how well the KGS authenticates users before issuing private keys. The idea of IBE was further improved to support much better systems. The concept of attribute-based, where ABE can be considered as a generalization of identity based encryption (IBE), where as mentioned earlier, the encryption is based on some identity. Thus, ABE is more expressive than IBE.

*2) Attribute based encryption (ABE):*The notion of ABE was first introduced by Sahai and Waters [7] as a new method for fuzzy identity-based encryption. In an ABE system, the plaintext is encrypted with a set of attributes. The KGS, which possesses the master key, issues different private keys to users after authenticating the attributes they possess. Thus, these private keys are associated with the set of attributes each user possesses. In its basic form, a user can decrypt a cipher text if and only if there is a match between the attributes of the ciphertext and the user's key. In ABE system, it have two variants [1][5].

*Key Policy ABE (KP-ABE):*A cipher text is associated with a set of attributes and a user's decryption key is associated with a monotonic tree access structure[5][8]. Only if the attributes associated with the cipher text satisfy the tree access structure, the user can decrypt the cipher text.

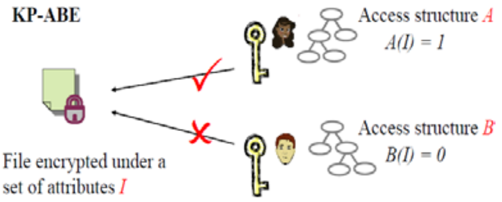


Fig. 1. Key-Policy Attribute-Based Encryption

integrators compose services for their customers. The service integrator provides a platform that lets independent service providers orchestrate and interwork services and cooperatively provide additional services that meet customers' protection requirements [6].

As shown in the figure 1, in KP-ABE, sender encrypts a message using a set of attributes. It defines an access structure, which is a threshold tree of the policy that sender wants to enforce. Receivers try to decrypt the message. The attributes receiver1 has satisfy the access structure and hence he can derive the key and decrypt the document. The attributes of receiver2 has do not satisfy the access structure and therefore cannot derive the key to decrypt the message. The key idea here is that the key is associated with the policy using an access structure.

Cipher text Policy ABE (CP-ABE):

The cipher text is encrypted with a tree access policy chosen by an encryptor, while the corresponding decryption key is created with respect to a set of attributes [5][8]. As long as the set of attributes associated with a decryption key satisfies the tree access policy associated with a given cipher text, the key can be used to decrypt the cipher text.

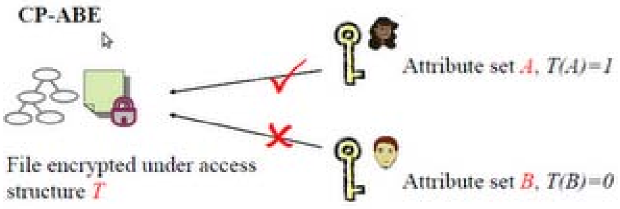


Fig 2 Cipher policy Attribute-Based Encryption

As shown in the diagram, CP-ABE reverses the role of encryption and key derivation. The encryption is associated with an access structure which is constructed using the policy. KGS simply issues private keys for the attributes users have. If users satisfy the owner defined access structure, they can decrypt it. The second variant is the encryption found in open systems as the cipher text is associated with the policy.

3) *Cipher text-Policy Attribute-Set Based Encryption (CP-ASBE)*:CP-ASBE allows users attributes to be organized into a recursive family of sets and policies that can selectively restrict decrypting users to use attributes from within a single set or allow them to combine attributes from multiple sets[1][4]. Thus, by grouping user attributes into sets such that those belonging to a single set have no restrictions on how they can be combined, CP-ASBE can support compound attributes without sacrificing the flexibility to easily specify policies involving the underlying singleton attributes. Similarly, multiple numerical assignments for a given attribute can be supported by placing each assignment in a separate set.

II. PROPOSED SYSTEM

We propose a serial attribute-set-based encryption scheme for access control in cloud computing. It extends the cipher text-policy attribute set-based encryption [5][8] with a hierarchical structure of system users, so as to achieve scalable, flexible and fine-grained access control. In this process, the cipher text is encrypted with a tree access policy chosen by an encryptor, while the corresponding decryption key is created with respect to a set of attributes. As long as the set of attributes associated with a decryption key satisfies the tree access policy associated with a given cipher text, the key can be used to decrypt the cipher text.

We have achieved fine grained access control and to achieve the assurances of cloud data integrity, availability and enforce the quality of cloud storage service, efficient methods that enable on-demand data correctness verification on behalf of cloud users have to be designed.

A. The Proposed System Design

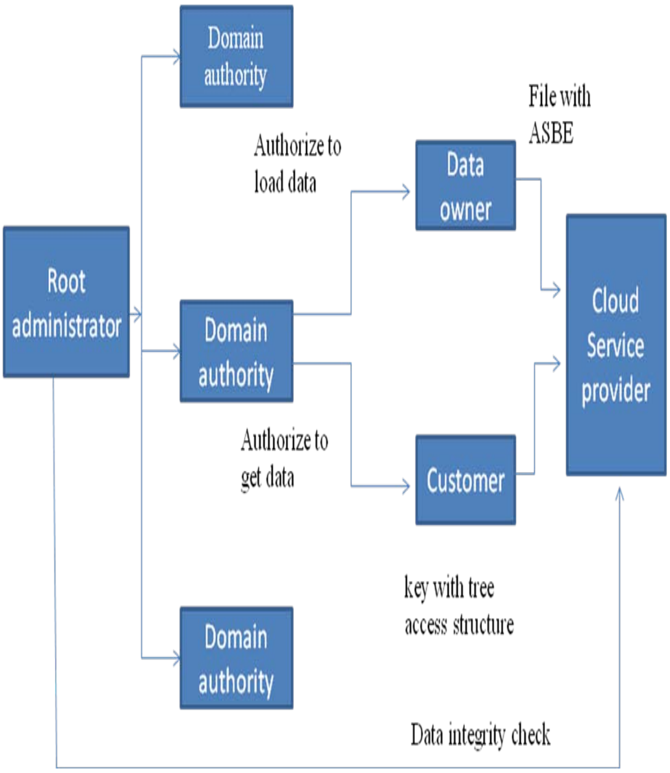


Fig3 System Model

B. Module Design and Description

1) *Root administrator and Domain Authority Registry*: Root authority holds the top most priority in the secure cloud storage and access system and it administrates the domain authority. Root authority has to register first in the cloud in order to get the services and to manage all the resources in the cloud. Next to root authority, Domain authority administrates the data owner who owns the data in the cloud.

2) *Bilinear Mapping:* Attribute based encryption is proceeded by bilinear mapping of attribute information of data owner and the data to be stored in the cloud. Bilinear mapping process achieved by multiplicative factors of both Logical AND operation and XOR operations. It is the process of pairing up the attribute information and thus cipher text policy ABE is processed.

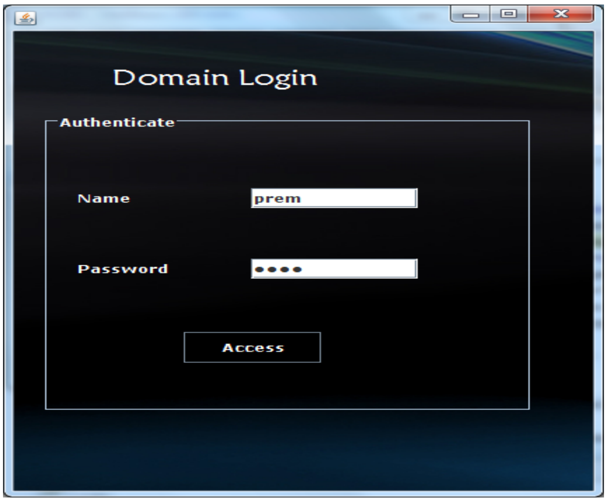
3) *Master and Secret key generation:* Master key is generated by doing the Logical AND operations of given attributes of data owner. Using the master key, public key is generated and secret key is generated by doing the logical XOR operations. Ciphering algorithms are applied using the secret key, Thus secured secret key is generated by Attribute based encryption

4) Secured Cloud Storage: Securities have been provided for the Data owner's file. These files are stored in the cloud servers. In order to do that the cloud server have to configure using VMware tool. In cloud servers crypto process was applied since client files are stored as secured files. For crypto process, we use Blowfish algorithm for the encryption and decryption process.

5) *Secured data retrieval:* In secured data retrieval module, the data are retrieved by the users upon the authentication of the hierarchical access control of Cloud system architecture. Data or keys are relocated in the cloud frequently depending upon the kind of data owner's identity and the data to be stored on the cloud. Based on the privilege of user they can retrieve their data. The privileges are given during the creation of tree access structure.

III. IMPLEMENTATION

The proposed system design is implemented using java and VM ware tool with mysql. The root administrator is responsible for generating and distributing root master keys and have a response to authorize the next level sub domain authorities. Each data owner first encrypts data files and then stores the encrypted data files on the cloud service provider. Each file is encrypted using algorithm BLOW FISH and which in turn encrypted with CP-ASBE. When a user sends request to domain authority, based on the access privilege for that user, the domain authority provide a encrypted file with tree access structure. Then the user can decrypt only if the key match with tree access structure. The Blowfish algorithm is 448 bits key length results in higher security, rather than using traditional DES and AES algorithms are smaller in key sizes results in lesser security. The data correctness of data in cloud service provider (CSP) must be checking using MD5 and Reed Solomon algorithm.

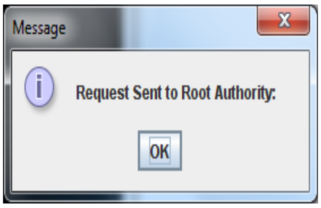


Name: prem

Password: ••••

Fig 4: New domain request

Here the new subordinate domain authority send request for join the trust authority to our root administrator.the root administrator verify wheather the new domain is valid



Request Sent to Root Authority:

Fig 5: Request sent root admin

The subordinate domain authority send its request to root administrator

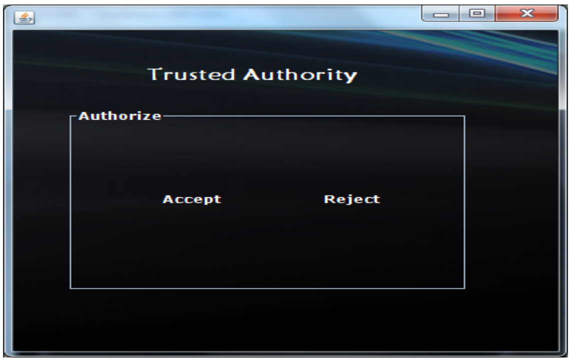


Fig 6: Root admin authorization

The root administrator verify wheather the new domain is valid or not andif it is valid then it send key access structure based on their privilage and provide unique id for the new trusted authority.

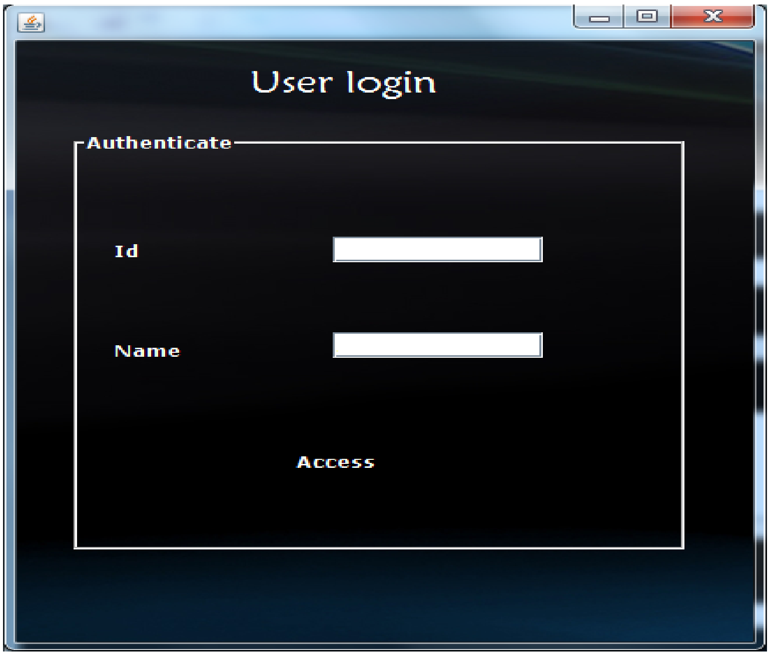


Fig 7: User login form

The trusted authority after authorized the data owner, the data owner can login to upload their data into cloud environment.

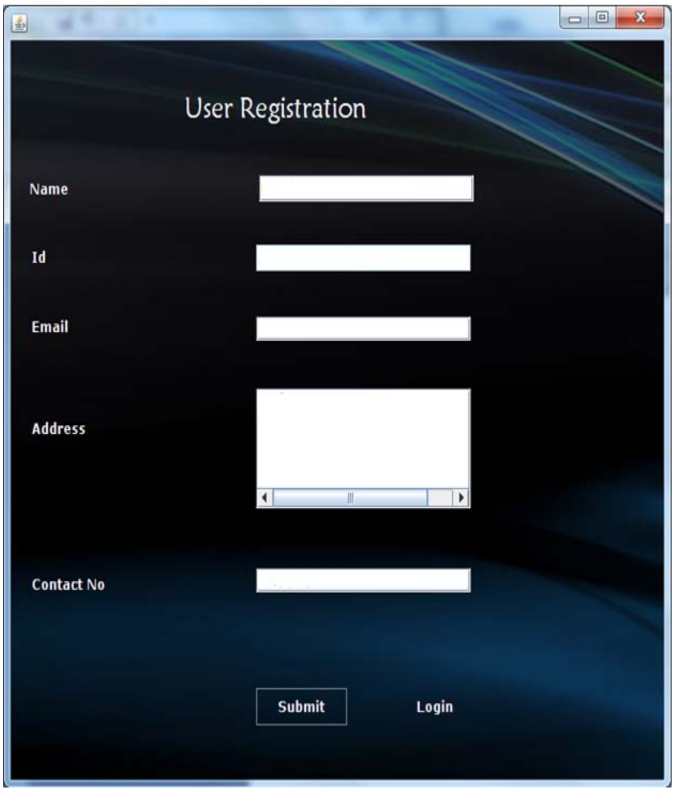
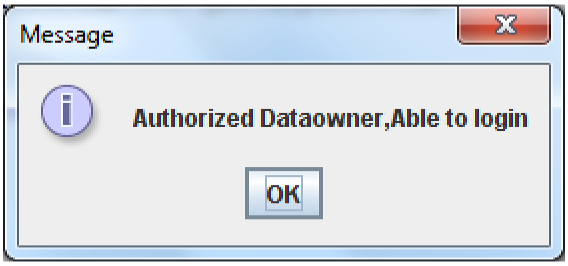


Fig 5: User registration from

Before uploading the data owners file it is necessary to get the details of data owner in registrations form and these details can be used for the purpose of key generation.



Authorized Dataowner,Able to login

Fig 5: login acknowledgment

The authorized data owner can get the acknowledgment response.

IV. CONCLUSION

We focus on improving the efficiency of ABE by leveraging a previously overlooked fact, i.e., the often-found hierarchy relationships among the Access control in that are inherent in many Cloud Computing Scenarios. As the first research effort along this direction, we coin the notion of hierarchical ABE (HABE), which can be viewed as the generalization of traditional ABE and to ensure the data owner's data being stored in the cloud is valid or not by check its Data integrity using by MD5 algorithm and Reed Solomon algorithm .This code is worked by adding extra information (redundancy) to original data .The encoded data are then transmitted to cloud service provider. If the code has any error, the added redundancy code will be used to detect which part of data is corrupted and correct them.

REFERENCES

[1] Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park. Computing Zhiguo Wan, Jun'e Liu, and Robert H. Deng, Senior Member, IEEE."A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing ",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, APRIL 2012

[2] 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.

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

[4] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Proc.ESORICS, Saint Malo, France, 2009.Sannella, M. J. 1994 Constraint Satisfaction and Debugging for Interactive User Interfaces. Doctoral Thesis. UMI Order Number: UMI Order No. GAX95-09398., University of Washington.

[5] 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.

[6] Hassan Takabi and James B.D. Joshi University of Pittsburgh Gail-Joon Ahn Arizona State University "Security and Privacy Challenges in Cloud Computing Environments" IEEE 2010,vol 1540-7993/10

[7] Sahai and B. Waters, "Fuzzy identity based encryption," in Proc .Acvances in Cryptology—Eurocrypt, 2005, vol. 3494, LNCS, pp.457–473.

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

[9] 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.

[10] H. Harney, A. Colgrove, and P. D. McDaniel, "Principles of policy insecure groups," in Proc. NDSS, San Diego, CA, 2001

[11] Amazon E lastic Compute Cloud (Amazon EC2) [Online]. Available: http://aws.amazon.com/ec2/

[12] Amazon Web Services (AWS) [Online]. Available: https://s3.amazonaws. com/

[13] 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/2099015