Volume No:1, Issue No:10 (March-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Enhanced Cloud Access Control Methodologies to Protect Sensitive and Policy Information by Hiding Attributes

Jerripothu Ravindra Babu
M.Tech Scholar,
Department of CSE,
Pydah College of Engineering,
Gambheeram, Visakhapatnam.

Mangalagiri Venkatesh
Assistant Professor,
Department of CSE,
Pydah College of Engineering,
Gambheeram, Visakhapatnam.

Dr.Ramesh Challagundla
Professor & Principal,
Department of CSE,
Pydah College of Engineering,
Gambheeram, Visakhapatnam.

Abstract:
Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services. Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Security and privacy are, thus, very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. User privacy is also required so that the cloud or other users do not know the identity of the user. In this paper, we propose the secure data storage in clouds for a new decentralized access. The cloud verifies the authenticity of the series without knowing the user's identity in the proposed scheme. Our feature is that only valid users can able to decrypt the stored information. It prevents from the replay attack. This scheme supports creation, modification, and reading the data stored in the cloud and also provide the decentralized authentication and robust. It can be comparable to centralized schemes for the communication of data, computation of data, and storage of data.

Keywords: Decentralized access, Access control, authentication of user, cloud storage, Privacy Preserving, Anonymous authentication.

Introduction:
Cloud computing allows application software to be operated using internet-enabled devices. Clouds can be classified as public, private, and hybrid. Cloud computing, or in simpler shorthand just "the cloud", also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand.

This can work for allocating resources to users. For example, a cloud computer facility that serves European users during European business hours with a specific application (e.g., email) may reallocate the same resources to serve North American users during North America's business hours with a different application (e.g., a web server). This approach should maximize the use of computing power thus reducing environmental damage as well since less power, air conditioning, rack space, etc. are required for a variety of functions. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications.The term "moving to cloud" also refers to an organization moving away from a traditional CAPEX model (buy the dedicated hardware and depreciate it over a period of time) to the OPEX model (use a shared cloud infrastructure and pay as one uses it).Proponents claim that cloud computing allows companies to avoid upfront infrastructure costs, and focus on projects that differentiate their businesses instead of on infrastructure.

Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand. Cloud providers typically use a "pay as you go" model. This can lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model.The present availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, and autonomic and utility computing have led to a growth in cloud computing. Companies can scale up as computing needs increase and then scale down again as demands decrease. The diagram represents the importance services of cloud computing i.e. Platform-as-a-service, Software/ Application as –a-service, Infrastructure as-a-service ,

Volume No:1, Issue No:10 (March-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Database – as- a- Service, Software plus – as –a- Service which plays a major role in public, private, hybrid ,community and combined cloud.

Figure 1: Cloud Services

Cloud computing exhibits the following key characteristics:

Agility improves with users' ability to re-provision technological infrastructure resources.

Cost reductions claimed by cloud providers. A public-cloud delivery model converts capital expenditure to operational expenditure. This purportedly lowers barriers to entry, as infrastructure is typically provided by a third party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained, with usage-based options and fewer IT skills are required for implementation (in-house). The e-FISCAL project's state-of-the-art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.

Device and location independence enable users to access systems using a web browser regardless of their location or what device they use (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.

Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

Performance is monitored, and consistent and loosely coupled architectures are constructed using web services as the system interface.

Productivity may be increased when multiple users can work on the same data simultaneously, rather than waiting for it to be saved and emailed. Time may be saved as information does not need to be re-entered when fields are matched, nor do users need to install application software upgrades to their computer.

Security and Privacy:

Cloud computing poses privacy concerns because the service provider can access the data that is on the cloud at any time. It could accidentally or deliberately alter or even delete information. Many cloud providers can share information with third parties if necessary for purposes of law and order even without a warrant. That is permitted in their privacy policies which users have to agree to before they start using cloud services. Solutions to privacy include policy and legislation as well as end users' choices for how data is stored. Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access.According to the Cloud Security Alliance, the top three threats in the cloud are "Insecure Interfaces and API's", "Data Loss & Leakage", and "Hardware Failure" which accounted for 29%, 25% and 10% of all cloud security outages respectively — together these form shared technology vulnerabilities. In a cloud provider platform being shared by different users there may be a possibility that information belonging to different customers resides on same data server. Therefore Information leakage may arise by mistake when information for one customer is given to other. Additionally, Eugene Schultz, chief technology officer at Emagined Security, said that hackers are spending substantial time and effort looking for ways to penetrate the cloud. "There are some real Achilles' heels in the cloud infrastructure that are making big holes for the bad guys to get into". Because data from hundreds or thousands of companies can be stored on large cloud servers, hackers can theoretically gain control of huge stores of information through a single attack — a process he called "hyperjacking".

RELATED WORK: Access control in clouds is gaining consideration on the grounds that it is imperative that just authorized clients have access to services. A colossal measure of data is constantly archived in the cloud, and much of this is sensitive data. Utilizing Attribute Based Encryption (ABE)[7], the records are encrypted under a few access strategy furthermore saved in the cloud.

Volume No:1, Issue No:10 (March-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Clients are given sets of traits and corresponding keys. Just when the clients have matching set of attributes, would they be able to decrypt the data saved in the cloud. Access control is likewise gaining imperativeness in on-line social networking where users store their personal data, pictures, films and shares them with selected group of users they belong. Access control in online social net-working has been studied in.The work done by "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems[9]," gives privacy pre-serving authenticated access control in cloud[10]. None-theless, the researchers take a centralized methodology where a single key distribution center (KDC) disperses secret keys and attributes to all clients. Unfortunately, a single KDC is not just a single point of failure however troublesome to uphold due to the vast number of clients that are upheld in a nature's domain. "Secure and effi-cient access to outsourced data," uses a symmetric key approach and does not support authentication.

Multi-authority ABE principle was concentrated on in "Improving privacy and security in multi authority attribute-based encryption [8]," in ACM Conference on Computer and Communications Security[9], which obliged no trusted power which requires each client to have characteristics from at all the KDCs.In spite of the fact that Yang et al. proposed a decentralized approach, their strategy does not confirm clients, who need to remain anonymous while accessing the cloud [10]. On the other hand, the approach did not provide client verification. The other weakness was that a client can make and store an record and different clients can just read the record. write access was not allowed to clients other than the originator. Time-based file assured deletion, which is initially pre-sented in [Perlman, "File System Design with Assured Delete," Proc. Network and Distributed System Security Symp[1] . Implies that records could be safely erased and remain forever difficult to reach after a predefined time. The primary thought is that a record is encrypted with an information key by the possessor of the record, and this information key is further encrypted with a control key by a separate key Manager.

PROPOSED SYSTEM:

Although we proposed a decentralized approach, their technique does not authenticate users, who want to re-main anonymous while accessing the cloud.

In an earlier work, proposed a distributed access control mechanism in clouds[1]. However, the scheme did not provide user authentication. The other drawback was that a user can create and store a file and other users can only read the file. Write access was not permitted to users other than the creator. In the preliminary version of this paper, we extend our previous work with added features that en-ables to authenticate the validity of the message without revealing the identity of the user who has stored informa-tion in the cloud. In this version we also address user re-vocation, that was not addressed. We use ABS scheme to achieve authenticity and privacy [10]. Unlike our scheme is resistant to replay attacks, in which a user can replace fresh data with stale data from a previous write, even if it no longer has valid claim policy. This is an important property because a user, revoked of its attributes, might no longer be able to write to the cloud. We, therefore, add this extra feature in our scheme and modify appropriately. Our scheme also allows writing multiple times which was not permitted in our earlier work.

ADVANTAGES OF PROPOSED SYSTEM:

•It provides authentication of users who store and modify their data on the cloud.
•It revoked users cannot access data after they have been revoked.
•Costs are comparable to the existing centralized ap-proaches.

SYSTEM ARCHITECTURE:

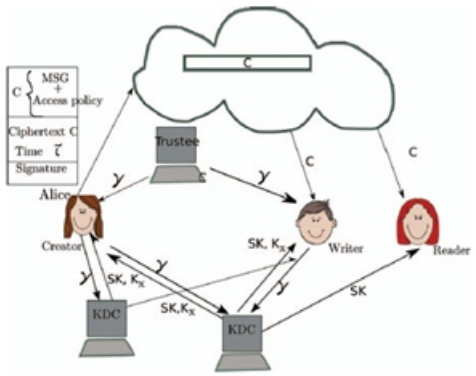

Figure 2: System Architecture

Volume No:1, Issue No:10 (March-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

PROPOSED METHODOLOGY

A. Distributed Key Policy Attribute Based Encryption:

KP-ABE is a public key[11] cryptography primitive for one-to-many correspondences. In KP-ABE, information is associated with attributes for each of which a public key part is characterized. The encrypton associates the set of attributes to the message by scrambling it with the comparing public key parts. Every client is assigned an access structure which is normally characterized as an access tree over information attributes, i.e., inside hubs of the access tree are limit doors and leaf hubs are connected with attributes. Client secret key is characterized to reflect the access structure so the client has the ability to decode a cipher-text if and just if the information attributes fulfill his access structure. The proposed scheme consists of four algorithms which is defined as follows.

Attribute Based Encryption(ABE):

in many applications, we find we need to share data according to an encryption policy without prior knowledge of who will be receiving the data. Suppose an administrator needs to encrypt a junior faculty member's performance review for all senior members of the computer science department or anyone in the dean's office. The administrator will want to encrypt the review with the access policy ("Computer Science" AND "Tenured") OR "Dean's Office". In this system, only users with attributes (credentials) that match this policy should be able to decrypt the document. The key challenge in building such systems is to realize security against colluding users. For instance, the encrypted records should not be accessible to a pair of unauthorized users, where one has the two credentials of "Tenured" and "Chemistry" and the other one has the credential of "Computer Science". Neither user is actually a tenured faculty member of the Computer Science Department. Proposed a solution to the above problem that they called Attribute-Based Encryption (ABE)[11]. In an ABE system, a party encrypting data can specify access to the data as a boolean formula over a set of attributes. Each user in the system will be issued a private key from an authority that reflects their attributes (or credentials). A user will be able to decrypt a cipher text if the attributes associated with their private key satisfy the boolean formula ascribed to the cipher text.

A crucial property of ABE systems is that they resist collusion attacks as described above.

Attribute Based Signature(ABS):

Identity-based signature[5] is a powerful mechanism for providing the authentication of the stored and transmitted information where the identity can be an arbitrary string such as an email address or a registration number, etc. While this is useful for applications where the data receiver knows specifically the identity of the data signer, in many applications the signer will want to have fine-grained control over how much of her personal information is revealed by the signature.A new vision of identity-based signature that they called Attribute-Based Signature (ABS), in which a signer is defined by a set of attributes instead of a single string representing the signer's identity. In ABS, a user obtains a set of attributes from one or multiple attribute authorities. An attribute-based signature assures the verifier that a signer, whose set of attributes satisfies a (possibly) complex predicate, has endorsed the message. The following example illustrates the concept. Suppose we have the following predicate:Professor OR (((Biology Department OR Female) OR above 50 years old) AND University A).

For example, Alice's attributes are (University A, Female). Bob's attributes are (above 50 years old, Professor). Although their attributes are quite different, it is clear that Alice and Bob can generate a signature on this predicate, and such a signature releases no information regarding the attribute or identity of the signer, i.e. Alice or Bob, except that the attribute of the signer satisfies the predicate. This kind of authentication required in attribute-based signatures differs from that offered by identity-based signatures. An ABS solution requires a richer semantics, including privacy requirements, similar to more recent signature variants like group signatures (Chaum; Heyst, 1991), ring signatures (Rivest; Shamir; Tauman, 2001),and mesh signatures (Boyen, 2007). All of these primitives share the following semantics:unforgeability. By verifying the signature, one is assured that the message was indeed endorsed by a party who satisfies the condition described in the claim. Privacy The signature reveals no information about the signer other than the fact that it satisfies the claim. In particular, different signatures cannot be identified as generated by the same party. Besides these two semantics,

Volume No:1, Issue No:10 (March-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

ABS has another important property which is called collusion resistance [4]. It assures different parties should not be able to pool together their attributes to sign a message with a claim which none of them satisfy alone. For instance, if Alice has an attribute Female, and her friend Bob has an attribute Professor, they should not be able to sign a message claiming to have both the attributes. ABS has found many important applications. For instance, it helps to provide fine-grained access control in anonymous authentication systems.

The Key Distribution Center(KDC):

Suppose once again that Bob and Alice want to communicate using symmetric key cryptography. Suppose they have never met and thus ha vet not established a shared secret key in advance. How can they now agree on a secret key, given that they can communicate with each other only over the network? A solution often adopted in practice is to use a trusted KDC. The KDC is a server that shares a unique secret symmetric key with each registered user. This key might be manually installed at the server when a user first registers. The KDC knows the secret key of each user, and each user can communicate securely with the KDC using this key. Let's see how knowledge of this one key allows a user to obtain a key securely for communicating with any other registered user. Suppose that Alice and Bob are users of the KDC; they know only their individual keys, KA–KDC and KB–KDC, respectively, for communicating securely with the KDC. Alice takes the first step, and they proceed as illustrated in Figure 8.19.

1. Using KA–KDC to encrypt her communication with the KDC, Alice sends a message
to the KDC saying she (A) wants to communicate with Bob (B). We
denote this message, KA–KDC (A, B) .
2. The KDC, knowing KA–KDC, decrypts KA–KDC (A, B) . The KDC then generates
a random number, R1. This is the shared key value that Alice and Bob will use
to perform symmetric encryption when they communicate with each other. This key is referred to as a one-time session key, because Alice and Bob will use this key for only this one session. The KDC now needs to inform Alice
SECURITY IN COMPUTER NETWORKS
Alice knows R1
Bob knows R1
Bob and Alice communicate using
symmetric session key R1
KDC
KA–KDC (R1, KB–KDC (A,R1))
KA–KDC (A,B)
KB –KDC (A,R1)
Setting up a one-time session key using a key distribution center Bob of the value of R1 . The KDC thus sends back a message to Alice, encrypted using KA–KDC, containing the following._ R1, the one-time session key that Alice and Bob will use to communicate. A pair of values, A and R1, encrypted by the KDC using Bob's key, KB–KDC. Denoted this KB–KDC (A, R1). It is important to note that KDC is sending Alice not only the value of R1 for her own use, but also an encrypted version of R1 and Alice's name, encrypted using Bob's key. Alice can't decrypt this pair of values in the message (she doesn't know Bob's encryption key), but then she doesn't really need to. We'll see shortly that Alice will simply forward this encrypted pair of values to Bob, who will be able to decrypt them. The KDC puts these items into a message, encrypts them using Alice's shared key, and sends them to Alice. The message from the KDC to Alice is thus KA–KDC (R1, KB–KDC (A, R1)).

3. Alice receives the message from the KDC, decrypts it, and extracts R1 from the message. Alice now knows the one-time session key, R1. Alice also extracts KB–KDC (A, R1) and forwards this to Bob.
4. Bob decrypts the received message, KB–KDC (A, R1) using KB–KDC and extracts A and R1. Bob now knows the one-time session key, R1, and the person with whom he is sharing this key, A.

Setup:

This algorithm takes as input security parameters and attribute universe of cardinality N. It then defines a bilinear group of prime number. It returns a public key and the master key which is kept secret by the authority party.

Encryption:

It takes a message, public key and set of attributes. It outputs a cipher text.

Key Generation:

It takes as input an access tree, master key and public key. It outputs user secret key.

Volume No:1, Issue No:10 (March-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Decryption:

It takes as input cipher text, user secret key and public key. It first computes a key for each leaf node. Then it aggregates the results using polynomial interpolation technique and returns the message.

B. File Assured Deletion:

The policy of a file may be denied under the request by the customer, when terminating the time of the agreement or totally move the files starting with one cloud then onto the next cloud nature's domain. The point when any of the above criteria exists the policy will be repudiated and the key director will totally evacuates the public key of the associated file. So no one can recover the control key of a repudiated file in future. For this reason we can say the file is certainly erased.To recover the file, the user must ask for the key supervisor to produce the public key. For that the user must be verified. The key policy attribute based encryption standard is utilized for file access which is verified by means of an attribute connected with the file. With file access control the file downloaded from the cloud will be in the arrangement of read just or write underpinned. Every client has connected with approaches for each one file. So the right client will access the right file. For making file access the key policy attribute based encryption.

Results:

Attributes hiding is to protect the sensitive and policy information of Authenticated user in Cloud. When Kdc is requested by the user then Kdc generates the Public key and Private key along with User details, which are known to users in cloud.

Figure 3 : Generating keys

Hence other users of cloud may steal sensitive Information to prevent this, hiding public and private keys concept was introduced. Once the key was received by the User, the message MSG is encrypted under the access policies and the access policies decide who can access the data stored in the cloud. The cipher text C with signature is c, and is sent to the cloud.

Figure 4: Uploading and Encrypting file

The cloud verifies the signature and stores the cipher text C. When a reader wants to read, the cloud sends C. If the user has attributes matching with access policy, The file can decrypt and get back original message. Using their access policies the users can download their files by the help of kdc's to issue the private keys for the particular users. After trustee token issuance for the users, the users produce the token to the KDC then the token verify by the KDC if it is valid then KDC will provide the public and Private key to the user. After users received the keys the files are encrypt with the public keys and set their Access policies.

Figure 5: Decrypted file

Conclusion:

Security can improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to

Volume No:1, Issue No:10 (March-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

solving security issues that many customers cannot afford to tackle. The proposed method is to secure cloud storage using decentralized access control with anonymous authentication which gives client renouncement also prevents replay attacks. The cloud does not know the identity of the client who saves data, however just checks the client's certifications. Key dissemination is carried out in a decentralized manner.

References:

[1] Sushmita Ruj, Member, IEEE, Milos Stojmenovic, Member, IEEE, and Amiya Nayak, Senior Member, IEEE, Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014

[2] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.-June 2012.

[3]Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In ACM Conference on Computer and Communications Security, pages 89{98, 2006. .

[4] Dan Boneh, Craig Gentry, and Brent Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In CRYPTO, pages 258{275, 2005.

[5] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," Proc. First Int'l Conf. Cloud Computing (CloudCom), pp.157-166, 2009.

[6]C. Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Stanford Univ., http://www.crypto.stanford.edu/craig, 2009.

[7] Nuttapong Attrapadung, Javier Herranz, Fabien Laguillaumie, Beno^_t Libert, Elie de Pana_eu,and Carla R_afols. Attribute-based encryption schemes with constant-size ciphertexts. Theor.Comput. Sci., 422:15{38, 2012.

[8] M. Chase. Multi-authority attribute-based encryption. In (To Appear) The Fourth Theory of Cryptography Conference (TCC 2007), 2007.

[9]F. Zhao, T. Nishide, and K. Sakurai, "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in ISPEC, ser. Lecture Notes in Computer Science, vol. 6672. Springer, pp. 83–97, 2011.

[10] S.Ruj , M..Stojmenovic and A . Nayak , "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 556–563, 2012.

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