A Cloud Based Authenticity Verification For Storing Data without Knowing User's Identity

K.Jyoshna srilakshmi
M.Tech Student,
Department of CSE,
Audisankara College of Engineering & Technology,
Gudur, Nellore (Dist), AP, India.

N.Lakshmi Chaitanya
Assistant Professor,
Department of CSE,
Audisankara College of Engineering & Technology,
Gudur, Nellore (Dist), AP, India.

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 purcha The term "moving to cloud" also refers to an organization moving away from a traditional CAPEX model (buy the dedicated sing licenses for different applications.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.

Cloud computing metaphor: For a user, the network elements representing the provider-rendered services are invisible, as if obscured by a cloud.

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 "hyper jacking".

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), the records are encrypted under a few access strategy furthermore saved in the cloud. 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 online 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 networking has been studied in [S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-based access control in social networks with efficient revocation," in ACM ASIACCS, 2011].

The work done by [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.] gives privacy preserving authenticated access control in cloud. Nonetheless, 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. The scheme In [W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in ACM Cloud Computing Security Workshop (CCSW), 2009.] uses a symmetric key approach and does not support authentication.

Multi-authority ABE principle was concentrated on in [M. Chase and S. S. M. Chow, "Improving privacy and security in multi authority attribute-based encryption," in ACM Conference on Computer and Communications Security, pp. 121–130, 2009.], 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. Ruj et al. proposed a distributed access control module in clouds. 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 presented in [Perlman, "File System Design with Assured Delete," Proc. Network and Distributed System Security Symp. ISOC (NDSS), 2007.], 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.

EXISTING SYSTEM:

Although we proposed a decentralized approach, their technique does not authenticate users, who want to remain anonymous while accessing the cloud. In an earlier work, proposed a distributed access control mechanism in clouds. 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 enables to authenticate the validity of the message without revealing the identity of the user who has stored information in the cloud. Inthis version we also address user revocation, that was not addressed. We use ABS scheme to achieve authenticity and privacy. 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.

DISADVANTAGES OF EXISTING SYSTEM:

• One limitation is that the cloud knows the access policy for each record stored in the cloud.
• It is unsecure.
• No privacy.
• Problem here is that the data records should have keywords associated with them to enable the search.

PROPOSED SYSTEM:

The ABE system is used to provide access control using attributes. Attributes may be anything. For example, it may person's roles or date. In ABE system the encryption phase consists of access rules. Rules are depended on the data owner and the consumer. It is not hidden in the existing systems. Through this, users can get the useful information from access rules without decryption. To improve the effectiveness of the ABE system, a new ABE algorithm is proposed. The proposed ABE algorithm has the features hiding Attributes and Access Policies. Through this, users getting useful information from the cipher text are avoided. Attributes and Access policies are hidden by the hash function and polynomial functions. The proposed ABE system ensures data privacy and policy privacy. Through this, the efficiency of the attribute based encryption system is improved. To improve ABE algorithm efficiency as well as ensuring the data secrecy and the policy secrecy.

ADVANTAGES OF PROPOSED SYSTEM:

•The ABE system which is secure in the form of data and also as the policies and attributes.
•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 decentralized approaches.

SYSTEM ARCHITECTURE:
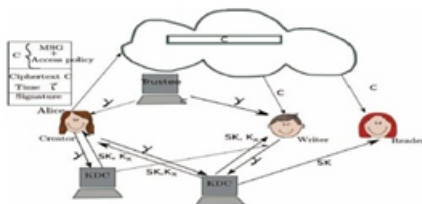
PROPOSED METHODOLOGY:
A. Distributed Key Policy Attribute Based Encryption:

KP-ABE is a public key 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 encryption 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.

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.

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

Conclusion:

The secure cloud storage using decentralized access control with anonymous authentication. The files are associated with file access policies, that used to access the files placed on the cloud. We have introduced a decentralized access control system 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. One limit is that the cloud knows the access strategy for each one record saved in the cloud. So To overcome the problem to using To improve the effectiveness of the ABE system, a new ABE algorithm is proposed. The proposed ABE algorithm has the features hiding Attributes and Access Policies.

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

[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] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing,"Proc. IEEE INFOCOM, pp.441-445, 2010.

[4] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc 14th Int'l Conf. Financial Cryptography and Data Security, pp. 136-149, 2010.

[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]A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-Based Cloud Computing," Proc. Third Int'l Conf. Trust and Trustworthy Computing (TRUST), pp.417-429, 2010.

[8]R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B.S. Lee, "Trustcloud: A Frameworkfor Accountability and Trust in Cloud Computing," HP Technical Report HPL-2011-38, http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html, 2013.

[9]R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 282-292, 2010.

[10]D.F. Ferraiolo and D.R. Kuhn, "Role-Based Access Controls," Proc.15th Nat'l Computer Security Conf., 1992.

[11]D.R. Kuhn, E.J. Coyne, and T.R. Weil, "Adding Attributes to Role-Based Access Control," IEEE Computer, vol. 43, no. 6, pp. 79-81,June 2010.

[12]M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf.

Authors Details:

K.Jyoshna Srilakshmi has received her B.Tech degree in Computer Science &Engineering from Jawaharlal Nehru Technological University, Anantapur, and is pursuing M.Tech in Computer Science & Engineering from the Audisankara College of Engineering and Technology (Autonomous),Gudur, Affiliated to the Jawaharlal Nehru technological university, Anantapur.

N.Lakshmi Chaitanya has received her B.Tech degree (Computer Science and Information Technology) from Annamacharya Institute of Technology and Sciences, Rajampet and M. Tech (Computer Science) from Narayana Engineering College. She is currently working as Assistant professor, in Audisankara College of Engineering and Technology, Gudur, AP, INDIA.