International Journal of Electrical Electronics & Computer Science Engineering
Volume 4, Issue 1 (February, 2017) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

A Novel Secure Data Storage with Unsigned Authentication in Cloud Computing used in Spread Access Control Framework

Nagarjuna Rao Gudelli, P Ravi Kumar
M.Tech Scholar, Assistant Professor, Dept. of CSE, Avanthi Institute of Engineering and Technology
ravikumarpodugu.phd@gmail.com

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 trans- action, 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 com- parable 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.***

I. 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 ex- ample, a cloud computer facility that serves European users during European business hours with a specific ap- plication (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

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 avail- able 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 in- stalled 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 informa- tion through a single attack — a process he called "hyper- jacking".

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 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 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 ASI- ACCS, 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 crypto- systems," 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 sym- metric 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 al- lowed 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.

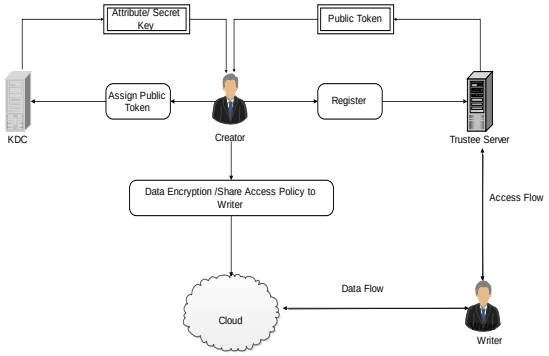
II. METHODOLOGY

Creator Module:

- A user first registers itself is one trustee; the trustee gives it a token and the signature and also signed with the trustees private key. The user on presenting this token obtains attributes and secret keys from one or more KDCs. After user encrypt the Data using ABE and upload to cloud.

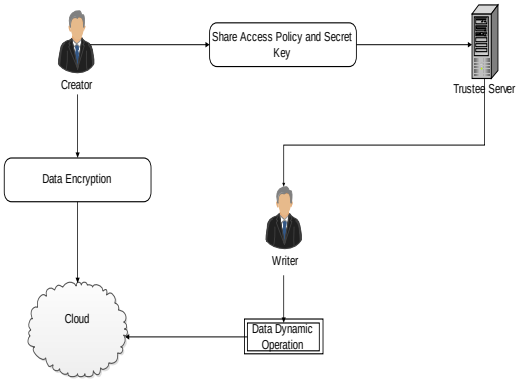
International Journal of Electrical Electronics & Computer Science Engineering
Volume 4, Issue 1 (February, 2017) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

- Creator to assign writes permission to the anonymous writer to authenticate the writer through Trustee.



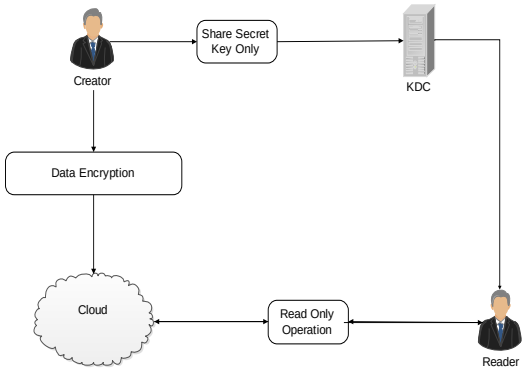
Data Dynamic Module:

- Write proceeds in the same way as file creation. By designating the verification process to the cloud, it relieves the individual users from time consuming verifications.
- A user can only write provided the cloud is able to validate its access claim. An invalid user cannot receive attributes from a KDC, if it does not have the credentials from the trustee. If a user's credentials are revoked, then it cannot replace data with previous stale data, thus preventing replay attacks.
- The Correct authenticated writer will modify the data that process data dynamic these are Insert, Delete, Update Operation will conducted.



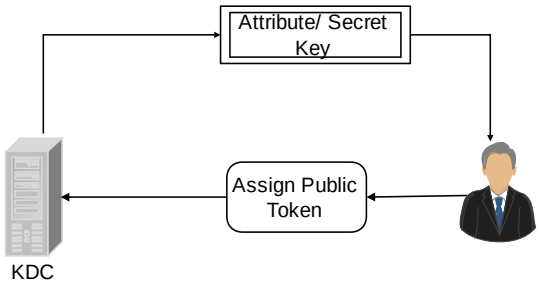
Read Only Module:

- A reader wants to read, the cloud sends C. If the user has attributes matching with access policy, it can decrypt and get back original message.
- Reader it tries to decrypt the data using the secret keys it receives from the KDCs. If it has enough attributes matching with the access policy, then it decrypts the information stored in the cloud.



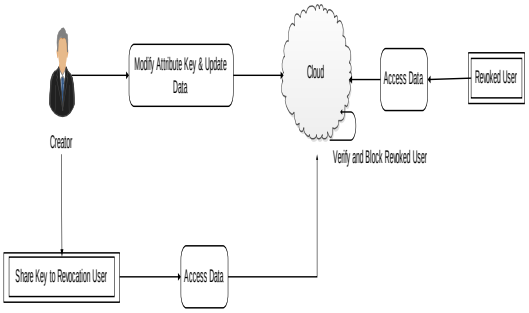
Key Distributed Centre Module:

- Authenticated user to assign a Trustee token and collect a public and private keys for encryption and decryption of the data.
- User receives a set of attributes from KDC and corresponding secret key. Note that all keys are delivered to the user securely using the user's public key, such that only that user can decrypt it using its secret key.



User Revocation:

- Now discuss how to handle user revocation Data Access. It should be ensured that users must not have the ability to access data, even if they possess matching set of attributes. For this reason, the owners should change the stored data and send updated information to other users.
- The set of attributes possessed by the revoked user is noted and all users change their stored data that have attributes. Revocation involved changing the public and secret keys of the minimal set of attributes which are required to decrypt the data.

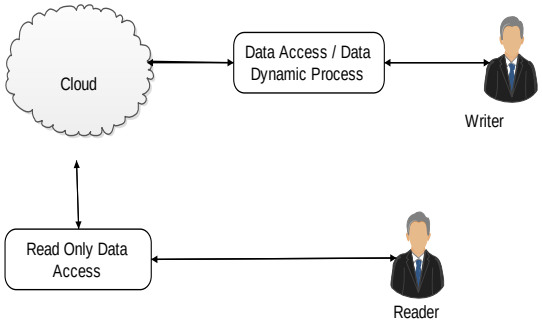


International Journal of Electrical Electronics & Computer Science Engineering
Volume 4, Issue 1 (February, 2017) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

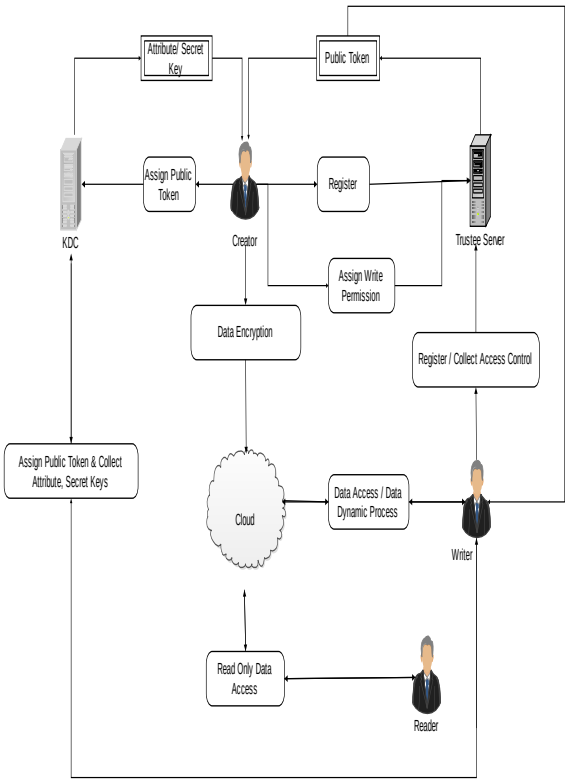
Cloud Storage Module:

Cloud Storage is an Internet service to store data in cloud. Google Cloud Storage allows world-wide storing and retrieval of any amount of data and at any time. It provides a simple programming interface which enables developers to take advantage of own reliable and fast networking infrastructure to perform data operations in a secure and cost effective manner. If expansion needs arise, developers can benefit from the scalability provided infrastructure.

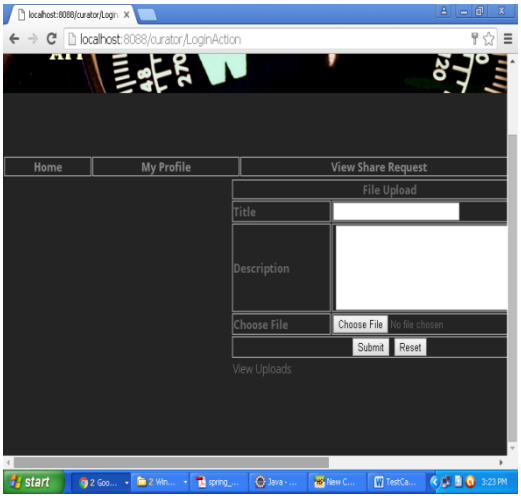
This module to store all data blocks and verification process over internet communication, cloud will automatically verify the signature when user request for data accessing process, user successfully verify after cloud server will return certain data to valid user.



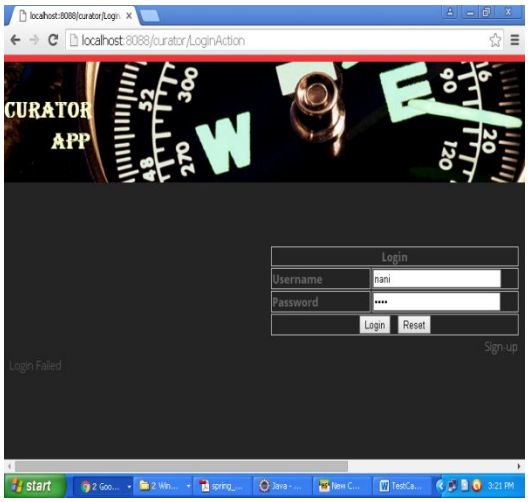
III. DATA FLOW DIAGRAM



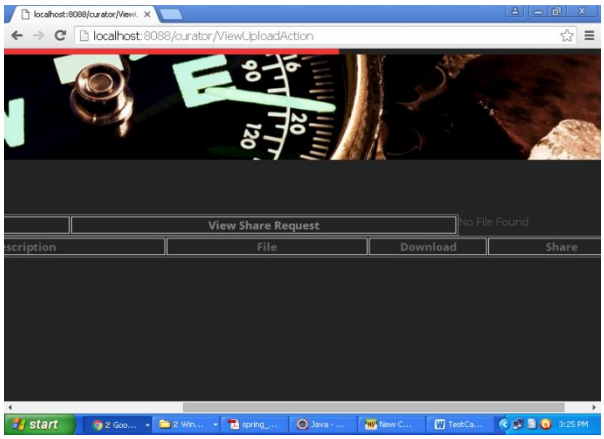
IV. DATA ANALYSIS



In Creator Login Page by Entering Correct User Name & Password



In Creator Login Page by Entering Incorrect User Name & Password



Failure in Uploading File

V. CONCLUSION

Presented a decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does

not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way. This project implements in windows azure cloud (Microsoft Cloud) storage and access through the real time web URL based application.

This system Architecture contains three modules users, a creator, a reader, and writer. Creator Alice receives a token from the trustee, who is assumed to be honest. A trustee can be someone like the federal government who manages social insurance numbers etc. On presenting her id (like health/social insurance number), the trustee gives her a token. There are multiple KDCs, which can be scattered. For example, these can be servers in different parts of the world. A creator on presenting the token to one or more KDCs receives keys for encryption/decryption and signing.

VI. REFERENCES

[1] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," Proc. IEEE/ACM Int'l Symp.Cluster, Cloud and Grid Computing, pp. 556-563, 2012.

[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 Framework for 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.