International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

Digital signature predicated and authentication distributed key management in Cloud computing.

H Prasanth Kumar[1]& P.Swathi[2]
[1]M-Tech sir.cv.Raman institute of Engg&Tech,Tadipatri,Anantapur(dist),JNTU-A,
Email Id: - hprasanth183@gmail.com
[2]Assist. Professor sir.cv.Raman institute of Engg&Tech,Tadipatri,Anantapur(dist),JNTU-A,
Email Id:- swathi.jaya53@gmail.com

Abstract:

Cloud computing is a elevating computing standard in which the computing framework is given as an accommodation over the Internet. The Cloud computing implement gives facility of data storage and access for cloud users, but when outsourcing the data to a third party causes safety issue of cloud data so data are for fended by restricting the data. We propose an incipient decentralized access control scheme for assure information storage in clouds that fortifies in nominate authentication. For achieving this goal, we propose a digital signature predicated authentication scheme with a decentralized architecture for distributed key management with multiple Key Distribution Centers. Homomorphism encryption scheme utilizing Paillier public key cryptosystem is utilized for encrypting the data that is stored in the cloud. Furthermore, our authentication plus access control scheme is decentralized and rich, dissimilar other access control schemes planned for clouds which are centralized. The communication, computation, and storage overheads are commensurable to centralized approaches.

Keywords: Cloud computing; digital signature predicated authentication; distributed key management

1. INTRODUCTION

Cloud Computing is the emerging technology where we can get software as an accommodation, platform as an accommodation and infrastructure as an accommodation. When it comes to storage as an accommodation, data privacy and data utilization are the primary issues to be dealt with. To handle the transaction of files to and from the cloud server, the files are encrypted afore being outsourced to the commercial public cloud. The storage maintains pertinent data and information work on how they will be carried out. Optimization on storage is predicated on how the storage facility avoided of unlike attacks and availableness of back-up. Cloud computing is invariably about consistency and availability of accommodation which will normally expect the storage to be usable all the time. Much of the data stored in clouds is extremely sensitive, for example,

medical records and convivial networks. Security and privacy are thus very paramount effects in cloud computing.

In one hand, the utilizer should authenticate itself afore initiating any transaction, and on the other hand, it must be ascertained that the cloud or other users do not ken the identity of the utilizer. The cloud can hold the utilizer accountable for the data it outsources, and likewise, the cloud itself accountable for the accommodations it provides. The validity of the utilizer who stores the data is withal verified. Apart from the technical solutions to ascertain security and privacy, there is additionally a desideratum for law enforcement. Cloud servers are prostrate to Byzantine failure, where a storage server can go wrong in arbitrary ways. The cloud is additionally prostrate to data change and server colluding attacks. In server colluding attack, ye adversary can compromise storage servers, so that it can change information files as long as they are internally consistent. To supply secure data storage, the data necessitates to be encrypted. However, the data is often modified and this dynamic property needs to be considered into account while planning efficient secure storage techniques.

A public cloud is one predicated on the standard cloud computing model, in which an accommodation provider builds resources, this as applications plus storage, available to the general public over the Internet. Public cloud accommodations may be free or offered on a pay-per-utilization model. A private cloud is a particular model of cloud computing that takes a discrete and assure cloud proclaimed environment in which only the showed client can operate. As with other cloud models, private clouds will supply calculating power as an adjustment among a virtualized environment using an fundamental pool of physical computing resource. However, under the private cloud model, the cloud (the pool of resource) is only accessible by a single organization supplying that organization on more preponderant control and secrecy. Hybrid cloud is a makeup of two or more clouds (private, community or public) that stay singular entities but are bound together, extending the gains of multiple deployment examples. By utilizing ―hybrid cloud‖ architecture, companies and individuals are able to obtain degrees of fault tolerance cumulated with locally quick usability without dependence on internet connectivity. Hybrid cloud architecture needs both on-site resources and off-site

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

(remote) server-predicated cloud base. Efficient search on encrypted information is still a paramount business in clouds. The clouds should not ken the query but should be capable to bring back the records that slake the query. This is achieved by denotes of searchable encryption. Access control in clouds is gaining care since it is paramount that only sanctioned users have access to valid accommodation. An abundance of data constitutes stored in the cloud, and much of this is sensitive data. Access control is withal gaining paramount in online convivial networking where users (members) store their personal information, pictures, and videos and apportion them with culled groups of users or communities they belong to. It is not just enough to store the contents securely in the cloud but it might withal be indispensable to ascertain anonymity of the utilizer. For example, a utilizer would relish to store some sensitive data but does not optate to be apperceived. The utilizer might want to post a comment on an article, but does not optate his/her identity to be disclosed. However, the utilizer should be able to prove to the other users that he/she is a valid utilizer who stored the data without revealing the identity.

2. RELATED WORK

Access control in clouds is earning consideration on the grounds that it is imperative that just approved clients have access to accommodations. A colossal measure of data is constantly archived in the cloud, and much of this is sensitive data. Utilizing Attribute connoted Encryption (ABE), the records are encrypted below a few access schemes furthermore saved in the cloud. Clients are given sets of traits and representing keys. Just when the clients have matching set of attributes, would they be able to decrypt the information preserved in the cloud. [9] [10] analyzed the access control in health care. The work done by [11] affords privacy preserving authenticated access control in the cloud. Nonetheless, the investigators take a centralized methodology where a single key distribution center (KDC) disseminates secret keys and attributes to wholly clients.

Haplessly, a individual KDC is not just a single point of loser, however onerous to uphold due to the prodigious number of clients that are upheld in a nature's domain [2]. The scheme In [12] utilizes a symmetric key approach and does not fortify authentication. Multi-ascendancy ABE rule was focused on in [13], which obliged no

believed power which needs each client to have features from at all the KDCs. Subsisting work on access control in the cloud are focused in universe. Except and, all other strategies use attribute predicated encryption (ABE). The scheme in utilizing a symmetric key approach and does not fortify certification.

The schemes do not strengthen certification as good. Earlier work by Zhao et al. Supplies privacy preserving authenticated access control in the cloud. Still, centralized approach where a single key distribution center (KDC) spreads secret keys and attributes to all users A single KDC is not just a single item of failure, but additionally it is arduous to maintain because of the sizeable voluminous number of users that are strengthened by the cloud environment [2]. Therefore, we emphasize that clouds should lead a decentralized approach while spreading secret keys and attributes of users. It is withal quite natural for clouds have many KDCs in different locations in the world. ABE was proposed by Sahai and Waters [7]. In the attribute proclaimed encryption, a user has a set of different attributes in integration to its unique ID. There are two classes of ABEs. In key-policy ABE or KP-ABE (Goyal et al. [8]), the sender has an access policy to encrypt data. An inditer whose attributes and set of keys have been revoked cannot indite back the data. The receiver amasses attributes and secret keys from the approved and is able to decrypt data if it has matching attributes.

In Ciphertext-policy, CP-ABE ([14], [3]), the receiver has the access policy in the form of a tree, with attributes as leaves and monotonic access structure with AND, OR and other threshold gates [2]. All the approaches take a centralized approach and sanction only one KDC, which is a single point of failure. Chase [13] proposed a multi ascendancy ABE, in which there are several KDC ascendant entities which spread attributes and secret keys to users. To ascertain innominate user authentication ABSs were introduced by Maji et al. [4]. This was a centralized approach. A recent schema by Maji et al. [5] takes a decentralized approach and provides authentication without disclosing the identity of the users. It is disposed to replay attack.

3. PROPOSED WORK

3.1 overview

The Fig.1 gives an overview of our proposed work. We fixate on amending upon two

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

main areas as discussed below. 3.1.1 Security Cognate Amendments:

1) We implement a decentralized architecture is implemented with multiple Key Distribution Centre (KDC) structure.

2) We implement a Role Predicated Access Control (RBAC) [15].

3) We achieve incognito authentication is achieved by implementing a vigorous digital signature algorithm(SHA -1 hash function) where the attributes of users are obnubilated from cloud [16].

4) The access policies that are set by users are obnubilated from other users by implementing Query driven approach.

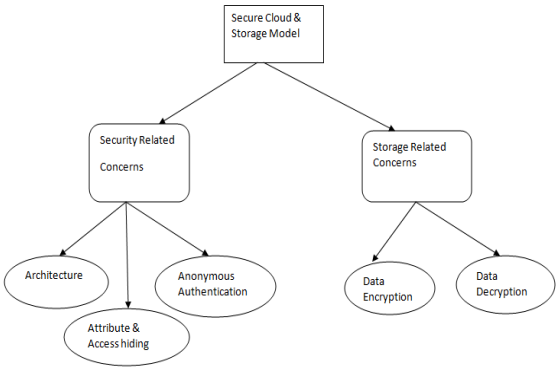

Fig.1. Overview of Proposed Work

1) For secure storage of data, we implement a vigorous encryption and decryption technique.

2) We utilize Homomorphic encryption technique where Paillier public key cryptosystem is utilized.

3) We implement automatic data retrieval in which string matching algorithm is utilized for recuperation of lost data.

3.2 PROPOSED SYSTEM ARCHITECTURE

The proposed architecture is a decentralized one where multiple numbers of KDCs are present for key distribution and management. These KDCs are geographically dispersed. In Fig.2 few users a scenario is presented with utilizer 1 as owner of the file, utilizer 2 as reader and utilizer 3 as inditer. These users are organized according to their roles predicated on their designation in the organization. If the utilizer 1 wants to upload his file to the cloud he first needs to get registered to his corresponding KDCs. The output of this registration process is the generation of a unique utilizer identifier for that utilizer by the KDC. This utilizer ID will be further utilized for all operations being performed by the utilizer in the cloud. First level of authentication is achieved by a registration process where the users are identified as a legitimate.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

Now the utilizer needs to go in for a second level authentication, which is done by the trustee system. The trustee can be postulated as a trusted third party such as a regime organization who uniquely identifies the users with some proof for instance, passport, vote id, driving license etc. This trustee system will engender a token for the utilizer once he engenders his unique Id to the trustee system. The engendered token is further passed on to the corresponding KDC for engendering the keys for encryption and decryption of the file that requires to be uploaded and/or downloaded.

For secure file storage, a Homomorphic encryption technique is adopted which implements an asymmetric key cryptography called Paillier Cryptosystem [17], [18]. This Cryptosystem is computationally vigorous and highly resistive to key-predicated attacks. It utilizes a series of involute mathematical functions for engendering a single parameter. Now the files are encrypted utilizing keys that are uniquely engendered for this file according the access policy that has been defined by the owner of the file. The file is encrypted with keys that are engendered by KDCs and withal predicated on the access policy that is defined for that utilizer by the owner of the file. Predicated on utilizer authentication and claim policy, the files are encrypted and stored in the cloud. Afore being encrypted, all files are encoded utilizing Base64 encoder and a facsimile of the pristine encrypted file is stored in backup files.

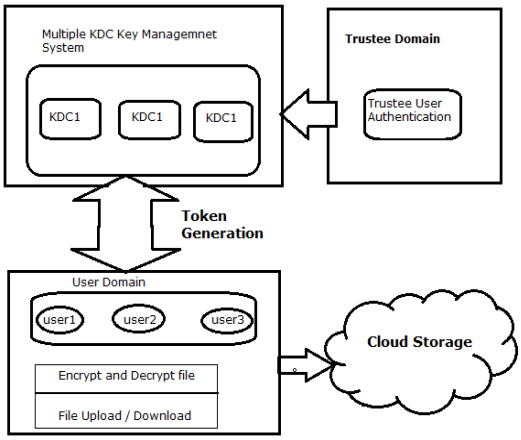

Fig.2. Overall View of Proposed Architecture

When some other utilizer in cloud is fascinated with reading or inditing the files, the access will be sanctioned predicated on the access policy defined for that particular utilizer. Homogeneous to the upload operation, the utilizer sends a request for downloading the file from the cloud. He is authenticated and keys for decrypting the files are obtained utilizing which the files are retrieved back. Afore being downloaded, the cloud checks for the integrity of the file. If the file is found to be corrupted or transmuted, it will perform an automatic

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

recuperation operation. The file recuperation process is carried out in two steps. First, the file's integrity is checked by utilizing a string matching algorithm. Then, if found to be corrupted it is then recuperated by file supersession of pristine file that is kept in backup.

3.3 PAILLIER CRYPTOSYSTEM

The Paillier cryptosystem, which is a type of public key cryptography, enables high security with symmetric key data encryption. One of the striking features of the asymmetric algorithm is that the key utilized for encryption are different from the key utilized for decryption, so that users have separate sets of private and public keys. The public key is made available widely whereas the private key is kept secret. The files are encrypted utilizing the pubic key but can be decrypted only utilizing the corresponding private key. Albeit the attributes of public and private keys are mathematically cognate but the private key cannot be derived from the public key.

The Table.1 presents the notations utilized in the Paillier algorithm. The algorithms for the Pallier system are given.

Table.1. Notations used in Algorithm

Symbols	Computation
$\mathbb{Z}n^{2*}$	set of integers co - prime to n^2
$\mathbb{Z}n*$	set of integers co - prime to n
$\mathbb{Z}n$	set of integers n

A) Key Generation

1) Choose two large prime numbers p and q, such that gcd (pq, (p-1) (q-1)) = 1.

2) Compute n = pq, λ = lcm (p-1, q-1).

3) Select random integer g such that $g \in \mathbb{Z}*^{n^2}$

4) Calculate the following modularmultiplicative inverse

5) μ = (L (gλ mod n2))-1 mod n, where thefunction L is defined as L(u) = u – 1/n.

6) The public (encryption) key is (n, g).

7) The private (decryption) key is (λ,).

B) File Encryption

1) Let m be a message to be encrypted where $m \in \mathbb{Z}n$.

2) Select random r where $r \in \mathbb{Z}*$.

3) Compute cipher text as, $c = gm \cdot r^n \bmod n^2$

C) File Decryption

1) Cipher text $c \in \mathbb{Z}* n^2$

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

2) Compute message, m = L(cλ mod n2) μ mod n

The Paillier Cryptosystem description

4. PERFORMANCE ANALYSIS

The efficiency of the system can be analyzed in terms of encryption and decryption time of the algorithm. We compare the performance of the system with a symmetric key encryption (3DES) system. In Table.4 shows the encryption and decryption time of different file size. From the Table.3 it is pellucid that the amount of encryption time taken by Paillier algorithm is virtually half as compared to that of 3DES algorithm for the same input. Similarly the amount of decryption time is additionally half when compared to 3DES algorithm.

We can visually perceive that the proposed system is at par with performance when compared to symmetric key predicated system when files of different size were given as input and encrypted. The results show the encryption and decryption time is expeditious when compared with the symmetric algorithm predicated system

Table.2. Performance analysis of 3DES and Paillier algorithm with varied File size

Input File Size (KB)	Encryption Time		Decryption Time	
	Symmetric Key Algorithm (3DES)	Asymmetric Key Algorithm (Paillier)	Symmetric Key Algorithm (3DES)	Asymmetric Key Algorithm (Paillier)
3	3.54	2.26	3.53	2.24
5	5.76	2.35	5.81	2.33
7	8.31	1.77	8.21	1.73
11	13.78	7.99	13.65	7.87
16	22.19	8.65	21.89	8.64
21	28.28	19.06	27.99	17.99

5. EXPERIMENTAL RESULT

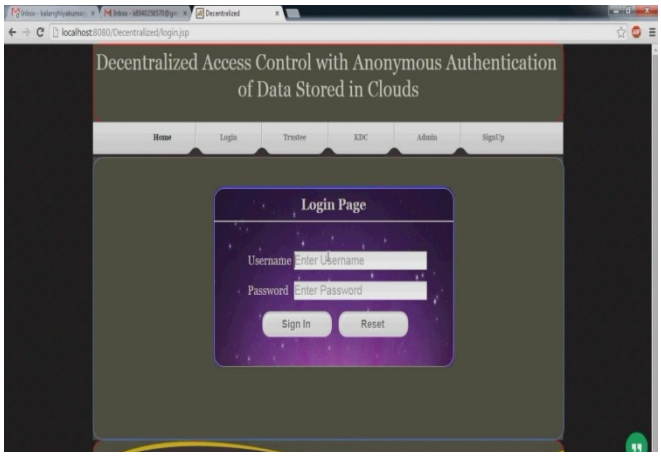

Fig 3:- Authentication Control

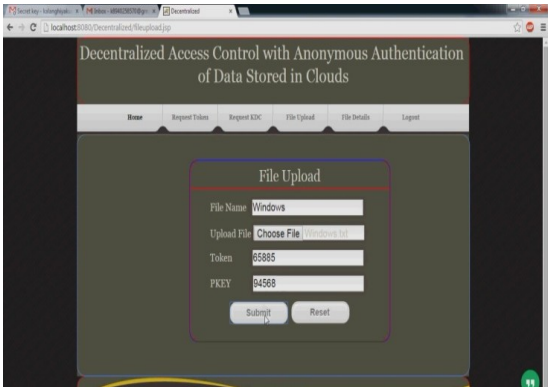

Fig 4:- Data Uploading

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

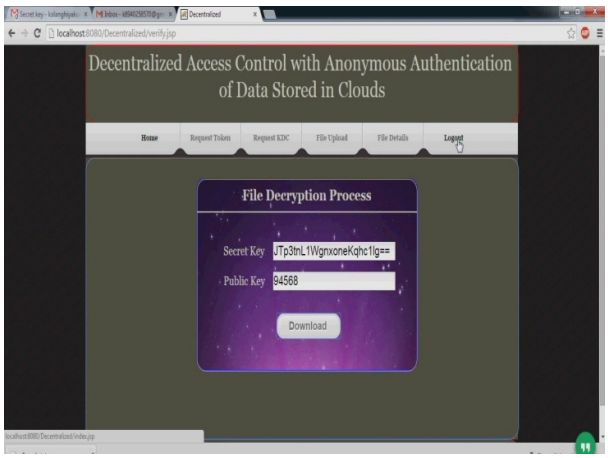

Fig 5:- key generation

6. CONCLUSION

In this paper, we addressed the security and storage issues simultaneously predicated on the type of architecture, access control methods and the authentication techniques. The key distribution is done in a distributed way by implementing multiple KDC structure. The users are anonymously authenticated and their attributes are obnubilated from the cloud by implementing digital signature algorithm. The access policies associated with individual files are obnubilated from other users by implementing a Query predicated approach. Further, storage cognate security issues are enhanced by implementing a Homomorphic encryption technique to encrypting the outsourced data. Additionally, the cloud servers are prone to sundry types of attacks that can cause data loss or leakage. This issue is addressed by implementing a string matching algorithm that detects deviations and automatically retrieves the lost data utilizing backed-up data.

6. REFERENCES

[1] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp 343-352, 2009.

[2] 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.

[3] Sushmita Ruj, Member, IEEE, Milos Stojmenovic, Member, IEEE, and Amiya Nayak, Senior Member, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds" IEEE,2014.

[4] M. Chase, "Multi-Authority Attribute Based Encryption," Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007

[5] A. Beimel, "Secure Schemes for Secret Sharing and Key Distribution," PhD thesis, Technion, Haifa, 1996.

[6] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data", ACM Cloud Computing Security Workshop (CCSW), pp. 55-66, 2009.

[7] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc.Ann. Int'l

Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "AttributeBased Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.

[9] Personal M. Li, S. Yu, K. Ren, and W. Lou, "Securing health records in cloud computing: Patient-centric and finegrained data access control in multi owner settings," in SecureComm, pp. 89–106, 2010.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ACM ASIACCS, pp. 261–270, 2010.

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

[12] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to [18] https://www.cs.cornell.edu, Accessed: 17 July 2014

[19] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

outsourced data," in ACM Cloud Computing Security Workshop (CCSW), 2009.

[13] 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.

[14] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp 321-334, 2007.

[15] Michael E. Whitman and Herbert J. Mattord, "Principles of Information Security", Cengage Learning, Fourth Edition, 2011

[16] William Stallings, "Cryptography and Network Security, Principles and Practice", Pearson Education, Fourth Edition, 2005

[17] William Stallings, "Cryptography and Network Security, Principles and Practice", Pearson Education, Fourth Edition, 2005.