ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Importance Shrinkage Rule with Objective Security and Data Represent in Cloud Storage

Vatsavayi Dharmaraju
M.Tech Student
Sri Vatsavayi Krishnam Raju College of Engineering & Technology
Bhimavaram, AP.

Dr.Penmetsa Vamsi Krishna Raja, M.Tech
Principal
Sri Vatsavayi Krishnam Raju College of Engineering & Technology
Bhimavaram, AP.

Abstract:
Cloud computing different model and feature the provides privacy security and access control challenges, the sharing of physical resources between unfrosted tenants. In order to achieve safe storage, policy based file access control, policy based file assured deletion and policy based renewal of a file stored in a cloud environment This Scheme prevents Replay attack which mean Eaves Dropping can be avoided Support Creation of data inside storage, Modifying the data by unknown users the propose system privacy data storage in clouds in new decentralized models The cloud security users the authenticity of different series indifferent data the user's identity in the proposed model. Our feature is the valid user is decrypt the stored information Time based file Revocation scheme is used for file assured deletion. When the time limit of the file expired, the file will be automatically revoked and cannot be accessible to anyone in future. Manual Revocation also supported. Policy based file renewal is proposed. The Renewal can be done by providing the new key to the existing file will remains the file until the new time limit reaches Homomorphism encryption scheme using Parlier public key cryptosystem is used for encrypting the data that is stored in the cloud. Broadcast re-encryption with TPA Our analysis supports delegation of private keys which subsumes Hierarchical Identity-Based Re-Encryption.

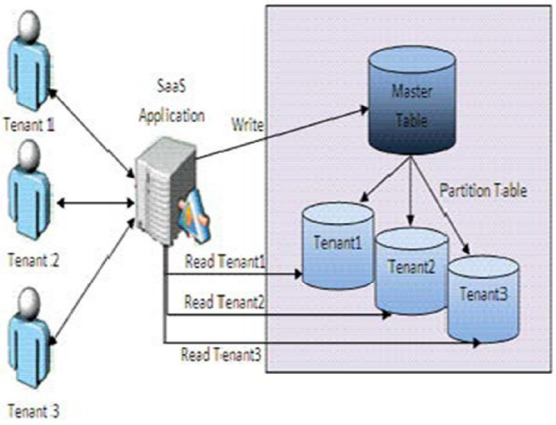
Index Terms: ***CLOUD STORAGE, RENEWAL POLICY, DECENTRALIZED ACCESS, POLICY BASED ACCESS***

INTRODUCTION

Cloud computing is new enabling same convenient and on-demand network model to destitute different configurable computing locations that rapidly provisioned and released with minimal manatees [1] errors service users interaction There is two main models of cloud structures public cloud and security cloud To take advantage of public clouds, data owners his data upload their data to commercial cloud service users which are usually considered to be semi trusted the , honest and curious In add cloud providers that specialized in a particular area can bring number of services in a single company might develop Some benefits to users include scalability reliability in efficiency Scalability is cloud computing take unlimited modeling and data storage capacity[2]

The cloud is reliable in that it new model access to applications and documents different locations in the world through the Internet Cloud computing is take considered as efficient because it take organizations to free up resources and to focus in sufficient and development items.

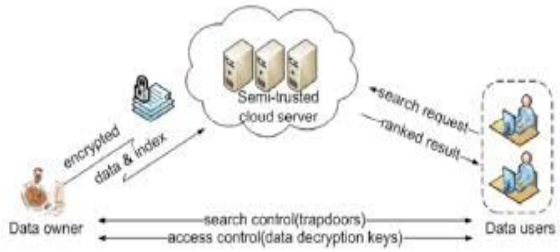
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



The first goal of our work is to implement anonymous authentication of users. In [1], the authors discuss anonymous [3] authentication of users and highlight its importance. The privacy settings of users must be followed in such a manner that the identity of the user should not become evident to either the cloud service providers or to other users. Thus, the anonymity of users is preserved Access control is essential when unauthorized users tries to access the data from the storage, so that only authorized users can access the data. It is also significant to verify that the information comes from a reliable source. We need to solve the problems of access control, authentication, and privacy protection by applying suitable encryption techniques given in [5] [6] [7]

RELATED WORK

The authors [12] take a centralized model is a single key distribution center (KDC) sharing secret keys and attributes to all the users.[4] insufficient a single KDC is a single data faults but difficult to maintain because of the large number of users that are supported in a cloud locations We used RSA algorithm for encryption/Decryption. This algorithm is the proven mechanism for secure transaction Here we are using the RSA algorithm with key size of 2048 bits. The keys are split up and stored in four different places.[5] If a user wants to access the file he/she may need to provide the four set of data to produce the single private key to manage encryption/decryption The client made request to the key manager for the public key, which will be generated according to the policy associated with the file. Different policies for files, public key also differs [6]for same public key for same policy will be generated. Then the client generates a private key by combining the username, password and security credentials. Then the file is encrypted with the public key and private key and forwarded to the cloud The private key for encrypt the file was generated with the combination of username, password and the answers for the security level questions.[7] After generating the private key the client will request to the key manager for the public k e y . The key manager will verify t h e policy associated with the file. If the policy matches with the file name then same public key will be generated [8]



PRIOR WORK

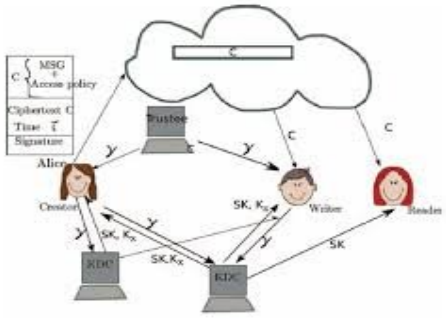
We now take a brief survey of the existing approaches for handling various security issues such as key distribution, access control and authentication The centralized architecture model implements a single Key Distribution Center (KDC) for key distribution as well as for incorporating security mechanism. Several existing works discuss about centralized access control mechanisms [5], [6], [7], [8], [17]. Though implementation of a single KDC structure is convenient, but it faces many potential problems [9] A critical problem is that of single point failure which is not at all desirable in a cloud environment where there are large numbers of active users. Significant overheads occur since a single KDC is used to distribute secret keys and attributes to all users. Furthermore the schemes discussed in [10] and [7] do not support authentication. In [10] the security system supports only single write and read operation. In view

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

of the above problems, a decentralized cloud approach is emphasized where the task of key management

A. DATA SECURITY

As discussed earlier, most of the data that are outsourced are sensitive in nature. They are stored in servers located externally in different locations. The cloud service providers should adopt and use strong cryptographic techniques for handling the data with utmost security and safety. Though the paper [11] presented a decentralized architecture with anonymous authentication the data access policies and attributes associated with individual users are not hidden from cloud In ABE, a user is provided with a set of attributes according to its unique ID. Attribute Based Encryption is classified as two classes. In Key-policy ABE or KP-ABE (Goyal et al.[17]), the sender has an access policy to encrypt the data . A writer whose attributes and keys have been revoked cannot write back the stale information[12] The receiver receives attributes and secret keys from the attribute authority and is able to decrypt the stored information if it has the matching attributes to access the data (refer fig1.b). In Cipher text-policy, CP-ABE ([21],[20]), 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



PROPOSED WORK

Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them. Authentications of users[13] who store and modify their data on the cloud .The Third party auditor give the permission to file stored in to cloud and if user problem means can block that user anonymous authentication is achieved. Our technique is the added feature and take control different valid users is able to security the stored data. Perform with public key and private key for file download process with multi KDC. Our authentication scheme is correct, collusion secure resistant to replay attacks, and protects privacy[14] of the user. To ensure anonymous authentication, a attribute based signature is used [12] Ensuring data security in cloud number of efficient data representative network model for cloud data storage in the third party auditor in trustful security for user to operate their data security in cloud storage [15]

A. Cryptographic Key Assumption

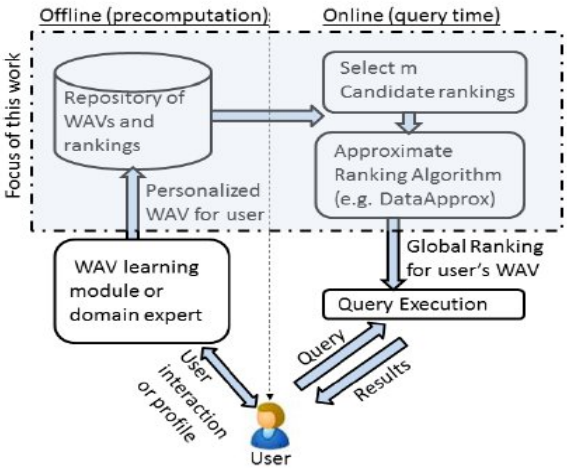
Symmetric-Key Encryption (SKE) These techniques usually efficient but introduce complexity in EHR systems as additional mechanisms are required to apply access control. In particular[16] all healthcare providers use one shared key for encryption and decryption if the shared key is compromised, all EHRs are compromised the Public-Key Encryption (PKE). These techniques provide a secure solution but are not practical for secure EHR storage due to the requirement for an expensive public-key infrastructure (PKI) to be maintained for distributing and managing public keys and digital certificates for all healthcare providers [17]

B. Key Issuing Secured Access

Escrow-Free Key Issuing Protocol for CP-ABE The KGC and the data storing different involved in the user key model protocol In the protocol a user is required to data the two items before taking a set of keys[18][5] The KGC is taken for authenticating a user and

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

different attribute keys to him the user is entitled to the attributes The secret key is generated in the secure 2PC protocol among the KGC and the data security center. They engage in the arithmetic secure 2PC protocol with master secret keys of their own and issue independent key components to a user. The secure 2PC protocol deters them from data each other master secrets so that none of them can generate the whole secret keys of a user owner. [19]

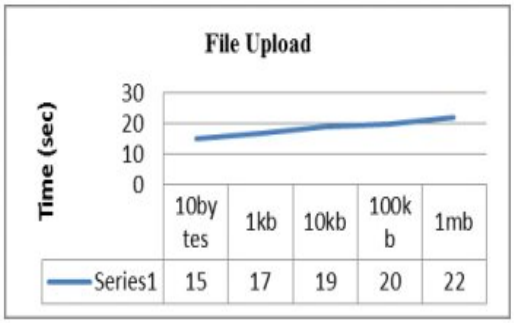


In Table.1, we show a comparison of a number of past approaches for access control with the scheme proposed by us. It is quite evident that our decentralized scheme given in the last row is powered by the maximum number of features. It has multiple read and multiple write access homomorphism encryption and performs anonymous authentication while hiding user attributes

Ref Paper	Architecture	Write/read access	Type of Encryption	Privacy preserving authentication	User Revocation
[6]	Centralized	1-W-M-R	Symmetric key cryptography	No Authentication	No
[7]	Centralized	1-W-M-R	ABE	No Authentication	No
[10]	Decentralized	1-W-M-R	ABE	No Authentication	Yes
[12]	Centralized	1-W-M-R	ABE	No Authentication	Yes
[8]	Decentralized	1-W-M-R	ABE	No privacy preservation	No
[1]	Decentralized	M-W-M-R	ABE	Authentication	Yes
Our Scheme	Decentralized	M-W-M-R	Homomorphic Encryption combined with ABE	Authentication with attribute based hidden policy	Yes

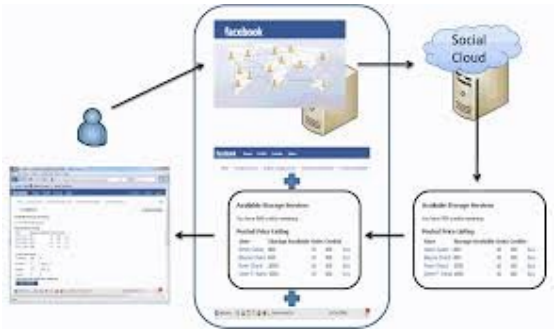
Legend: W- Write, M- Multi, R- Read, ABE- Attribute Based Encryption [1,6]

The performance of this paper was analyzed under various file sizes. At first the time performance of this paper is evolved for different file sizes. Then the cryptographic operation time is evolved. The only achievement of this paper is, it supports random time duration for any size of files to download



C. Security Related Improvements:

We implement a decentralized architecture is implemented with multiple Key Distribution Centre (KDC) structure [1]We implement a Role Based Access Control (RBAC) [11] We achieve anonymous authentication is achieved by implementing a strong digital signature algorithm where the attributes of users are hidden from cloud [13] The access policies that are set by users are hidden from other users by implementing Query driven approach The file is encrypted with keys that are generated by KDCs and also based on the access policy that is defined for that user by the owner of the file.[20] Based on user authentication and claim policy, the files are encrypted and stored in the cloud. Before being encrypted, all files are encoded using Base64 encoder and a copy of the original encrypted file is stored in backup files



ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

We developed a prototype model of proposed system and executed it as a cloud application by connecting 10 computer nodes using intranet. To host the developed application, we used the freeware eye OS private cloud application platform that provides web based desktop interface to run the system [19]. Since our model is based on RBAC access control method, it follows strictly designation based control and distinguished power. We developed an application for universities where the hierarchical roles of dean, secretary, principal, professors, assistant professors, lecturers and students have defined access rights according to their respective role[21]

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 modular multiplicative inverse
5) $\mu = (L (g^{\lambda} \bmod n^2))^{-1} \bmod n$, where the function 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, $c = g^{m} \cdot r^{n} \bmod n^2$

C) File Decryption

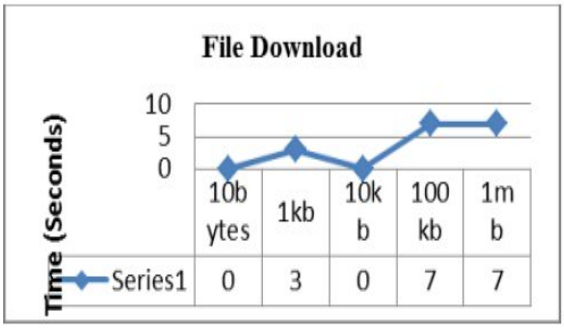
1) Cipher text $c \in \mathbb{Z}^{*}_{n^2}$
2) Compute message, $m = L(c^{\lambda} \bmod n^2)\ \mu \bmod n$

DISCUSSION

Our proposed scheme is compared with other access control schemes and show that our work supports many features that the other schemes did not support.Our proposed work is robust and decentralized, most of the others are centralized in nature. Our work also supports privacy preserving authentication, which is not being supported by others. We compare the computation and communication[8] costs incurred by the users and clouds and show that our distributed approach has comparable costs to centralized approaches. The most expensive operations involving pairings and is done by the cloud Thus the proposed system is fast and secure in terms of file recovery and file encryption. The time required to find the files been corrupted is also fast and the recovery of corrupted files back to original takes reduced amount of time.[13]

Download File

Downloading time is also not a constant one. For same size file the time taking for downloading is randomly different.[9] Using the time taken to download the file one can identify the encryption standard. To confuse the hacker the random time delay is achieved.



CONCLUSION

We propose 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 It is a Decentralized access of system in which every system have the access control of data . The Cloud which is a Secured storage area where the anonymous authentication is used, so that only the permitted users can be accessed The policy renewal is made as easy as possible. The renew key is added to the file. Whenever the user wants to renew the files he/she may directly download all renew keys and made changes to that keys, then upload the new renew keys to the files

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

stored in the cloud Finally a message digest of the UID is generated using SHA-1 and the file to be uploaded is encrypted using Pallier cryptosystem. In this manner, a three way authentication is achieved The limitation of this scheme is that the cloud knows the access policy that is being used for each record stored in the cloud. In future, we would like to hide the access policy of a user from the cloud The challenging problem is the construction of KP-ABE scheme with constant cipher text size and constant private key size

FUTURE WORK

In future the file access policy can be implemented with Multi Authority based Attribute based Encryption. Using the technique we can avoid the number of wrong hits during authentication. Create a random delay for authentication, so the hacker can confuse to identify the algorithm Its provides user revocation and prevents to the replay attacks. The cloud do not know the identity of the user who store the information, but one and only verifies the user's credentials we can avoid the number of wrong hits during authentication. Create a random delay for authentication, so the hacker can confuse to identify the algorithm.

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] Yang Tang, Patrick P.C. Lee, John C.S. Lui and Radia Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion", IEEE Transcations on dependable and secure computing, VOL. 9, NO. 6, NOVEMBER/DECEMBER 2012

[3] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in ACM CCS, , pp. 735–737, 2010

[4] Y. Tang, P.P.C. Lee, J.C.S. Lui, and R. Perlman, "FADE: Secure Overlay Cloud Storage with File Assured Deletion," Proc. Sixth Int'l ICST Conf.Security and Privacy in Comm. Networks (SecureComm), 2010

[5] R. Perlman, "File System Design with Assured Delete," Proc. Network and Distributed System Security Symp. ISOC (NDSS), 2007

[6]. 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.

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

[8]. 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.

[9]. 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.

[10]. 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

[11]. F. Zhao, T. Nishide, and K. Sakurai, "Realizing FineGrained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems," Proc. Seventh Int'l Conf. Information Security Practice and Experience (ISPEC), pp. 83-97, 2011.

[12]. A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005.

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

[14]. G. Wang, Q. Liu, and J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services," Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737, 2010

[15] www.cis.syr.edu/~wedu, Accessed on: 9 July 2014.

[16] http://en.m.wikipedia.org/wiki/Discretionary_access_contr ol, Accessed on: 13 July 2014.

[17] https://www.cs.cornell.edu, Accessed: 17 July 2014.

[18] www.cs.rit.edu, Accessed on: 20 July 2014.

[19] Eye OS Applications, www.eyeos-apps.org, Accessed on: 3 September 2014.

[20]. Mohamed Nabeel, Member, IEEE, Ning Shang, and Elisa Bertino, Fellow, IEEE," Privacy Preserving PolicyBased Content Sharing in Public Clouds" IEEE Transactions on Knowledge and Data Engineering, Vol. 25, No. 11, November 2013.

[21]. A.B. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 568-588, 2011.

Author details

Vatsavayi Dharmaraju is one of the author received B.Tech (CSE) Degree from JNTU Kakinada in 2012. He is studying M.Tech inSri Vatsavayi Krishnam Raju College of Engineering & Technology, Bhimavaram, AP.

Dr.Penmetsa Vamsi Raja, He did his PhD from JNTU Kakinada AP. He received M.Tech Post Graduation degree in C.S.T department from Andhra University, Visakhapatnam, A.P. He is presently working as Principal in Sri Vatsavayi Krishnam Raju College of Engineering & Technology Bhimavaram AP. He has authored more than 20 relevant publications in journals and Conferences. His Research areas include Computer Networks, Network Security, Cloud Computing, Big Data, Data Mining and Software Engineering.