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

Reducing Overhead Costs to Data Owners Along With Data Confidentiality in Cloud Computing Using Encryption Technique

Sirisha Yegamamidi
M.Tech,
Department of CSE,
Sarada Institute of Science Technology & Management, Srikakulam.

Behara Vineela
Assistant Professor,
Department of CSE,
Sarada Institute of Science Technology & Management, Srikakulam.

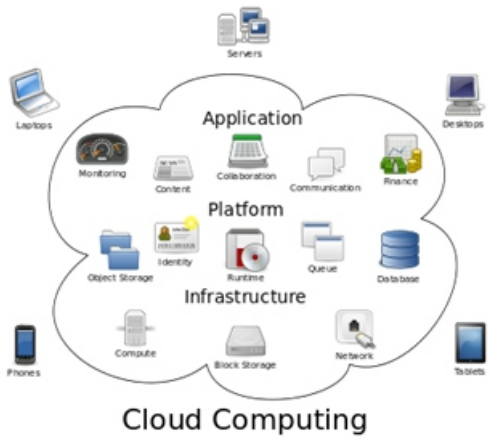
Abstract:

Cloud computing is playing an important role for sharing data through group of member. By sharing data in a group of people it will be consider mainly security and privacy of sharing data. To provide security and privacy of data the cloud technologies provides encryption of stored data. However, whereas encryption assures the confidentiality of the data against the cloud, the use of conventional encryption approaches is not sufficient to support the enforcement of fine-grained organizational access control policies. In this paper we are proposed secret key share signature schema for the verification of users and prime order xor group key generation is used for the generation group key. For the purpose data encryption and decryption we are using advanced encryption standard. By implementing those concepts we can provide authentication of users and also provide data security in the cloud.

Keywords: Privacy, Cloud computing, data sharing, policy decomposition, privacy preserving, access control, Two layer encryption

Introduction:

In a cloud computing system, there's a significant workload shift. Local computers no longer have to do all the heavy lifting when it comes to running applications. The network of computers that make up the cloud handles them instead. Hardware and software demands on the user's side decrease. The only thing the user's computer needs to be able to run is the cloud computing system's interface software, which can be as simple as a Web browser, and the cloud's network takes care of the rest.



The increased use of cloud computing services such as Gmail and Google Docs has pressed the issue of privacy concerns of cloud computing services to the utmost importance. The provider of such services lie in a position such that with the greater use of cloud computing services has given access to a plethora of data. This access has the immense risk of data being disclosed either accidentally or deliberately. Privacy advocates have criticized the cloud model for giving hosting companies' greater ease to control—and thus, to monitor at will—communication between host company and end user, and access user data (with or without permission). 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.

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

Solutions to privacy in cloud computing include policy and legislation as well as end users' choices for how data is stored. The cloud service provider needs to establish clear and relevant policies that describe how the data of each cloud user will be accessed and used. Cloud service users can encrypt data that is processed or stored within the cloud to prevent unauthorized access. Cryptographic encryption mechanisms are certainly the best options. In addition, authentication and integrity protection mechanisms ensure that data only goes where the customer wants it to go and it is not modified in transit.Strong authentication is a mandatory requirement for any cloud deployment. User authentication is the primary basis for access control, and specially in the cloud environment, authentication and access control are more important than ever since the cloud and all of its data are publicly accessible. CloudID provides a privacy-preserving cloud-based and cross-enterprise biometric identification solutions for this problem. It links the confidential information of the users to their biometrics and stores it in an encrypted fashion. Making use of a searchable encryption technique, biometric identification is performed in encrypted domain to make sure that the cloud provider or potential attackers do not gain access to any sensitive data or even the contents of the individual queries. 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.

Related Work:

Mohamed Nabeel and Elisa Bertino, proposed a paper [1] "Privacy preserving delegated access control in public cloud", these afford efficient group key management scheme that supports expressive ACPs. It assures the confidentiality of the data and preserves the privacy of users from the cloud while delegating most of the access control enforcement to the cloud. Here two layer encryption is performed, one by data owner and another one by cloud. Under our approach, the data owner performs a coarse-grained encryption, where cloud performs a fine-grained encryption on top of the owner encrypted data. A major issue is how to decompose access control policies (ACPs) such that the two layer encryption can be performed. Our approach is based on a privacy preserving attribute based key management scheme that protect the privacy of users while enforcing attribute based ACPs. Here decomposing the ACPs and utilize the two layer of encryption decrease the transparency at the Owner.

Mohamad Nabeel Dept. of Computer Science., Purdue Univ., West Lafayette, IN, USA, proposed a paper [2] "Privacy preserving delegated access control in the storage as a service model". Here a new approach for delegating privacypreserving fine-grained access enforcement to the cloud. The approach is based on a recent key management scheme that allows users whose attributes satisfy a certain policy to derive the data encryption keys only for the content they are allowed to access from the cloud. His approach preserves the confidentiality of the data and the user privacy from the cloud, where delegating most of the access control enforcement to the cloud. Additionally, in order to reduce the cost of re-encryption required whenever the access control policies changes, these approach uses incremental encryption techniques.Elisa Bertino, Mohamed Nabeel proposed a paper [5] "Towards attribute based group key management". Attribute based system permit fine-grained access control among a group of users each identified by a set of attributes. A protected collaborative applications need such flexible attribute based systems for managing and distributing group keys. These system able to support any monotonic access control policy over a set of attributes. When the group changes, the rekeying operations do not affect the private information of existing group members and thus our schemes eliminate the need of establishing expensive private communication channels.Nesrine Kaaniche, Maryline Laurent proposed a paper [6] "A Secure Client Side Deduplication Scheme in Cloud Storage Environments", here a new client-side deduplication scheme for securely storing and sharing outsourced data via the public cloud that towards the security and privacy of the public cloud environments. Here originality of proposal system is twofold. First, it ensures better confidentiality towards unauthorized users. Therefore every client compute a per data key to encrypt the data that he intends to store in the cloud. As such, the data access is managed by the data owner. Second, by integrate access privileges in metadata file, an authorized user can decode an encrypted file only with his private key. These solution is also shown to be resistant to unauthorized access to data and to any data disclosure during sharing procedure, given that two levels of access control verification.

EXISTING SYSTEM:

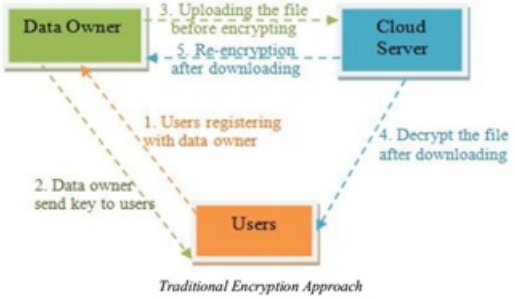
Many organizations have today ACPs regulating which users can access which data; these ACPs are often expressed in terms of the properties of the users, referred to as identity attributes, using access control

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

languages such as XACML. Such an approach, referred to as attribute based access control (ABAC), supports fine-grained access control which is crucial for high-assurance data security and privacy. Supporting ABAC over encrypted data is a critical requirement in order to utilize cloud storage services for selective data sharing among different users. Notice that often user identity attributes encode private information and should thus is strongly protected from the cloud, very much as the data themselves.Approaches based on encryption have been proposed for fine-grained access control over encrypted data. Those approaches group data items based on ACPs and encrypt each group with a different symmetric key. Users then are given only the keys for the data items they are allowed to access. Extensions to reduce the number of keys that need to be distributed to the users have been proposed exploiting hierarchical and other relationships among data items

DISADVANTAGES OF EXISTING SYSTEM:

•As the data owner does not keep a copy of the data, when ever user dynamics changes, the data owner needs to download and decrypt the data, re-encrypt it with the new keys, and upload the encrypted data. The user dynamics refers to the operation of adding or revoking users. Notice also that this process must be applied to all the data items encrypted with the same key. This is inefficient when the data set to be re-encrypted is large.
•In order to issue the new keys to the users, the data owner needs to establish private communication channels with the users.
•The privacy of the identity attributes of the users is not taken into account. Therefore the cloud can learn sensitive information about the users and their organization.
•They are either unable or inefficient in supporting fine-grained ABAC policies.



Traditional Encryption Approach

PROPOSED SYSTEM:

Now a day's security and privacy concern an important for cloud technologies for data storage. So that by implementing this approach the major concerned is encryption of stored data. However by implementing encryption process assures the confidentiality of the data against cloud. So that by using those conventional approaches are not sufficient to support the enforcement of fine-grained organizational access control policies. That is if the users credential will be changed the data owner will create new key and re encrypt data stored into cloud. So that by performing those approach the data owner incur high communication and computation cost. So that this problem can be overcome by implementing propose system. The proposed system mainly contains three concepts i.e signature generation, group key generation and encryption of the stored data. The implementation procedure of those concepts as follows.

Hybrid Encryption Approach

ADVANTAGES OF PROPOSED SYSTEM:

This approach has many advantages.
•When user dynamics changes, only the outer layer of the encryption needs to be updated. Since the outer layer encryption is performed at the cloud, no data transmission is required between the data owner and the cloud.
•Further, both the data owner and the cloud service utilize a broadcast key management whereby the actual keys do not need to be distributed to the users.
•Instead, users are given one or more secrets which allow them to derive the actual symmetric keys for decrypting the data.

Secret key share signature schema:

In this process the users and trusted center will communicate each other. By implementing this approach the trusted center will generate signature for each user of authentication purpose. After performing authentication

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

each user will get one secret key for the decryption process and secret key common for all group members. The implementation process secret key share signature schema as follows.

1.Each user select two prime number that is P, G and choose one private key a.
2.Each user calculate public key base on this formula pub=ga mod P
3.After calculate public keys the users will sent those public keys to trusted center.
4.The trusted center randomly choose Pi , gi and private keys of each users i.e ai.
5.After choosing the those values the trusted center will generate public key of each users by using this formula .

Pub=giai mod Pi

6.After generating public keys of each user the trusted center will those keys individual users.
7.The users retrieve the public key coming from the trusted center and calculate shared key by using this formula.

Shared key=puba mod P

8.After generating shared key of individual users will sent to trusted center.
9.The trusted center will retrieve those shared key and calculate group key by using this formula.
Secret key=sharedkey1 ^ sharedkey2 ^….. ^sharedkeyn.
10.Before sending secret key the trusted center will generate signature for individual users by using this formula.

Val=secret key ^ shared keyi
Sig=hash (Val)

11.After generating signature the trusted center will sent to individual users.
12.The users retrieve signature and again generate signature compare both signatures.
If both are equal user will get the secret key.
13.The trusted center will also sent that secret data owner.

Prime order xor group key generation schema:

After completion of authentication process the trusted center again generate group key by using following process.

1.After completion authentication each user randomly generate secret id(Pi), secret share(Si) and those values sent to trusted center.
2.The trusted center will retrieve those value from the user and random generate group key.
3.After generate group key the trusted center will generate shared values of each users by using following formula.

xi =k/ (Pi ^ Si)
yi =k Mod (Pi ^ Si)

4.The generated secret shares(xi,yi) of sent to individual users .
5.Each user will retrieve secret share and get secret key by using following formula
Secret key=xi *((Pi ^ Si) + yi

By performing these process all users will get the same secret. Before sending secret shares the trusted center will also sent secret key to data owner for the purpose second time encryption data.

File upload and encryption:

The data owner will upload the file into cloud service. Before uploading file the data owner will retrieve all secret keys from the trusted center. Here the data owner will encrypt the uploaded file two time. So that by performing encryption process in two time we improve security and privacy the stored data. By performing encryption process the data owner will use advanced encryption standard for getting cipher data. After performing encryption process the data owner will stored data into cloud service.

File download and decryption:

If user wants retrieve any file from the cloud service and get selected file in form of cipher data. After retrieving content file the user will perform decryption process in two times and get the original plain text. By performing decryption process the user will advanced encryption standard decryption process and get the plain text. Identity Provider maintains the metadata of encrypted data with details like filename, public key and secret key along with user privilege and attacker details also maintained in this system and also deals with creating new data owner and users. Identity Provider will create new data owner by providing details like username, validity and file size allowed.

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

According to the Data owner roles i.e. admin, doc etc the Identity Provider will provides the permission like upload file, account notification, audit logs and file deletion. Cloud Server system maintains all data owner files with following details like filename, cloud IP address, public key and private key. Particular data owner file also can be seen by providing file name. Even cloud server module can have the permission to modify any particular data owner file. Blocked users information is also maintained in this system.There are various advantages with the implementation of our system. When user is revoked, only access control encryption needs to be updated. No data transmission is required between data owner and cloud. No need to establish private communication channel with users for issue new keys. Assures the confidentially of the data and preserves the privacy of user from the cloud. This system also helps in Minimization computation cost.

CONCLUSION:

In this paper, we present a unique method for privacy preserving of data storage in multi-cloud environment. It also provides several advancements in cloud computing due to its technical capabilities. The feature work may also involves load-balancing in multi-cloud environment for maximum storage and accuracy for various users. Cloud computing is a growing paradigm as an enabling technology to deliver on-demand and elastic storage and computing capabilities, while removing the ownership need for hardware. But several privacy and security act demand strong protection of the cloud users, which in turn increases the complexity to develop privacy-preserving cloud services. The privacy preserving using delegated access control in multi-cloud delivers the critical capabilities required for a robust, cost-effective, and secure cloud security implementation.

References:

1. M. Nabeel and E. Bertino, "Privacy preserving delegated access control in public cloud," in IEEE Transactions on Knowledge and Data Engineering, 2014.

2. M. Nabeel and E. Bertino, "Privacy preserving delegated access control in the storage as a service model" in IEEE International Conference on Information Reuse and Integration (IRI), 2012.

3. M. Nabeel and E. Bertino, "Privacy preserving policy based content sharing in public clouds,"In IEEE Transactions on Knowledge and Data Engineering, 2012.

4. M. Nabeel, E. Bertino, M. Kantarcioglu, and B. M. Thuraisingham, "Towards privacy preserving access control in the cloud," in Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Work sharing, ser. Collaborate Com '11, 2011,pp. 172–180.

5. M. Nabeel and E. Bertino, "Towards attribute based group key management," in Proceedings of the 18th ACM conference on Computer and communications security, Chicago, Illinois, USA, 2011.

6. Nesrine Kaaniche, Maryline Laurent," A Secure Client Side Deduplication Scheme in Cloud Storage Environments" 6th International Conference on new Technologies, Mobility and Security year 2014.

7. D. Harnik, B. Pinkas, and A. Shulman-Peleg. Side channels in cloud services: Deduplication in cloud storage. IEEE Security And Privacy, 8(6):40–47, 2010.

8. A.Fiat and M. Naor, "Broadcast Encryption," Proc. 13th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '93), pp. 480-491, 1994.

9. D. Hankerson, A. J. Menezes, and S. Vanstone. Guide to Elliptic Curve Cryptography. Springer-Verlag New York, Inc., Secaucus, NJ, USA,2003.

10. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attri-bute-Based Encryption," Proc. IEEE Symp. Security and Privacy (SP '07), pp.321-334, 2007.

11. E. Bertino and E. Ferrari, "Secure and Selective Dissemination of XML Documents," ACM Trans. Information and System Security, vol. 5, no.3, pp. 290-321, 2002.

12. J. Camenisch, M. Dubovitskaya, and G. Neven, "Oblivious Trans-fer with Access Control," Proc. 16th ACM Conf. Computer and Comm.Security (CCS '09), pp. 131-140, 2009.

13. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of

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

Encrypted Data," Proc. 13thACM Conf. Computer and Comm. Security (CCS '06), PP 89-98, 2006.

14. J. Xu, E.-C. Chang, and J. Zhou. Weak leakage-resilient client-side deduplication of encrypted data in cloud storage. In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, ASIA CCS '13, pages 195–206, New York, NY, USA, 2013. ACM.

15. R. C. Merkle. A digital signature based on a conventional encryption function. In A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, CRYPTO '87, pages 369–378, London, UK, UK, 1988. Springer-Verlag.

16. R. C. Merkle. A digital signature based on a conventional encryption function. In A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, CRYPTO '87, pages 369–378, London, UK, UK, 1988. Springer-Verlag.

17. Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud" March 2012.

18. Junzuo Lai, Robert H. Deng, Chaowen Guan, and Jian Weng "Attribute- Based Encryption with Verifiable Outsourced Decryption" 2013.

Author's Details:

Sirisha Yegamamidi, is student in M.Tech(CSE) in Sarada Institute of Science Technology and Management, Srikakulam. He has received his B.Tech(IT) from Nimra Institute of Science and Technology (NIST), Vijayawada. she interesting areas are Network security & Software Engineering.

Behara Vineela, is working as Asst.professorinSarada Institute of Science, TechnologyAndManagement,Srikakulam, Andhra Pradesh. He received his M.Tech (CSE) from AITAM ,Tekkali,Srikakulam, AndhraPradesh. JNTU Kaki¬nada Andhra Pradesh.His research areas include Net¬work Security.