International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 12, December 2015
Available at http://internationaljournalofresearch.org

Key-aggregate Cryptosystem for reliable data Outsourcing among Cloud Storage

[1]SK.John Shaida & [2]U.Usha Rani

[1]M.Tech (CSE), Priyadarshini Institute of Technology & Science
[2] Associate Professor (Dept.of CSE), Priyadarshini Institute of Technology & Science

Abstract-

Cloud computing technology is widely used so that the data can be outsourced on the cloud can access easily. Different members can share that data through different virtual machines but present on the single physical machine. But the thing is user don't have physical control over the outsourced data. The need is to share data securely among users. In this paper, we proposed a novel scheme that provides secure data storage and retrieval. Along with the security, the access policy is also hidden for hiding the user's identity. This scheme is so powerful since we use key aggregation using the secure crypto algorithm. The novelty is that one can aggregate any set of secret keys and make them as compact as a single key, but concluding the power of all the keys being aggregated. The scheme detects any change made to the original file and if found clear the error's. And also address the number of cipher texts usually grows rapidly without any restrictions. So we have to reserve enough cipher text classes in another hand we need to expand the public-key. Although the parameter can be downloaded with cipher texts, it would be better if its size is independent of the maximum number of cipher text classes

Keywords: Aggregate key cryptosystem; Cloud storage; data sharing; key-aggregate encryption

1. INTRODUCTION:

In current era Data sharing is a significant functionality in cloud storage. For instance, bloggers can let their associate's opinion a subset of their cloistered pictures; an enterprise may fund her employee's admission to a quota of sensitive data. The thought-provoking problem is in what way we can efficiently share encrypted data. Obviously users can download the encrypted data from the storage, decrypt them, then direct them to others for sharing, but it drops the value of cloud storage. Therefore the users should be capable to give the access rights of the sharing data to others so that they can access these data from the server unswervingly. Cloud computing is widely increasing technology; data can be saved on cloud remotely and can have access to huge applications with quality services which are shared among customers. As increase in outsourcing of data the cloud computing serves does the management of data [1]. Its flexible and cost optimizing characteristic motivates the end user as well as enterprises to store the data on cloud. The insider attack is one of security concern which's needs to be focused. Cloud Service provider need to make sure whether audits are held for users who have physical access to the server. As cloud service provider stores the data of different users on same server it is possible that user's private data is leaked to others. The public auditing system of data storage security in cloud computing provides a privacy-preserving auditing protocol [2]. It is necessary to make sure that the data integrity without compromising the anonymity of the data user. To ensure the

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 12, December 2015
Available at http://internationaljournalofresearch.org

integrity the user can verify metadata on their data, upload and verify metadata

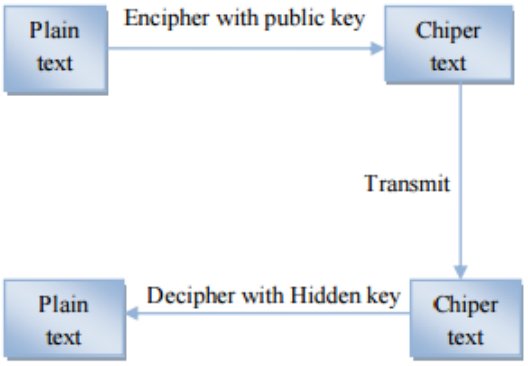

Fig. 1. Cryptosystem

Then there are 2 critical ways 1. Alice encrypt whole picture with one encryption key and give secret key to bob. 2. Encrypt all picture with special key and send corresponding secret key to bob. Sharing information is main task of cloud. For example, bloggers can want their personal photo. Organization grants permission for this personal data. But problem is sharing of the encrypted data and effectiveness of that task. Take another example of dropbox for explanation. Alice can collect personal picture on dropbox and she thinks no one can watch her photos. Due data loss possibility Alice does not feel secure and she encrypts all picture using own key before uploading. Another day her friend wants all pictures of the year in which bob appear. Alice use share option of dropbox but problem is that how to delegate decryption rights to bob.

2. A KEY-AGGREGATE ENCRYPTION SCHEME

A key-aggregate encryption scheme consists of five polynomial-time algorithms.

Setup The data owner executes the setup phase for an account on server which is not trusted. The setup algorithm only takes implicit security parameter.

KeyGen This phase is executed by data owner to generate the public or the master key pair (pk, msk).

Encrypt this phase is executed by anyone who wants to send the encrypted data. Encrypt (pk, m, i), the encryption algorithm AES takes input as public parameters pk, a message m, and i denoting ciphertext class. The algorithm encrypts message m and produces a ciphertext C.

Extract This is executed by the data owner for delegating the decryption power to the users by providing his Aggregate Decryption key.

Decrypt this is executed by the candidate who has the decryption authorities. Decrypt (kS, S, i, C), the decryption algorithm takes input as public parameters pk, a ciphertext C, i denoting ciphertext classes for a set S of attributes.

For example Alice wants to upload her data on the server. First she need to Setup an account on the server with security level parameter(1) and ciphertext classes(n) and then the public(pk) and master-secret key(msk) is generated by KeyGen algorithm. The data and index are encrypted by Alice as Encrypt (pk,i,m). If Bob wants to access her data on cloud he need to know an Aggregate key. Alice's master-secret key is used to compute the aggregate key by performing Extract (msk,S). Then Bob can be able to download the data from the server by Decrypt (Ks,S,i,Ci).

3. LITERATURE SURVEY

In 2006 V. Goyal, O. Pandey, A. Sahai, and B. Waters, worked on ―Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data‖, this paper develops a new cryptosystem for fine-grained sharing of encrypted data. This scheme was called Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt [4]. Advantages:-- Applicability of KP-ABE scheme is to sharing of audit-log information and broadcast encryption

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 12, December 2015
Available at http://internationaljournalofresearch.org

In 2007 F. Guo, Y. Mu, Z. Chen, and L. Xu,worked on ―Multi-Identity Single-Key Decryption without Random Oracles,‖ This Paper produce Multi-Identity Single-Key Decryption (MISKD).It is an Identity-Based Encryption (IBE) system where a private decryption key can map multiple public keys (identities). More exactly, in MISKD, a single private key can be used to decrypt multiple cipher texts encrypted with different public keys associated to the private key [3]. Advantages Multi-Identity Single-Key Decryption scheme is more efficient in decryption.

In 2009 J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, worked on ―Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,‖ .This system build an efficient system that allows patients both to share partial access rights with others, and to perform searches over their records. We formalize the requirements of a Patient Controlled Encryption scheme, and give several instances, based on existing cryptographic primitives and protocols, each achieving a different set of properties [2].
Advantages The patient can easily grant access to a category Similarly, doctors can add subcategories with arbitrary names, without assistance from the patient. This will be particularly useful if we can't predict the names of all possible subcategories, If a doctor needs to add a category for a new type of test, or if categories are labeled by visit dates.

In 2009,M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, worked on ―Dynamic and Efficient Key Management for Access Hierarchies,‖. The proposed solution has the following properties: (i) only hash functions are used for a node to derive a descendant's key from its own key; (ii) the space complexity of the public information is the same as that of storing the hierarchy; (iii) the private information at a class consists of a single key associated with that class; (iv) updates (revocations, additions, etc.) are handled locally in the hierarchy; (v) the scheme is provably secure against collusion; and (vi) key derivation by a node of its descendant's key is bounded by the number of bit operations linear in the length of the path between the nodes[1]. Advantages The dynamic scheme achieve a worst- and average-case number of bit operations for key derivation that exponentially better than the depth of a balanced hierarchy.
To reduce or block replay attack we use string matching algorithms[3][5] which is more efficient and perfect in security. It works more efficient than all other matching algorithms.

4. SYSTEM OBJECTIVE

The Objective of the system is to provide best solution for the Existing problem is that Alice encrypts files with distinct public-keys, but only sends Bob a single (constant-size) decryption key while sharing the files cipher text class index also considerable when a same user shares multiple files class index remain constant i.e no variation in class index. Since the decryption key should be sent via a secure channel and kept secret, small key size is always desirable. Using the Public-key Cryptosystem (public key Encryption algorithm)

PROBLEM DEFINITION:-

The challenging problem is how to effectively same user share multiple encrypted files thus class index remains same (constant). Of course users can download the individual or bulk encrypted files from the storage, decrypt them, then send them to others for sharing, but it loses the value of cloud storage. Users should be able to delegate the access rights of the sharing data to others so that they can access these data from the server directly

SCOPE:-

We Can protect users' data privacy is a central question of cloud storage. With more mathematical tools, cryptographic schemes are getting more versatile and often involve multiple keys for a single application. In this paper, we consider how to "compress" secret keys in

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 12, December 2015
Available at http://internationaljournalofresearch.org

public-key cryptosystems which support delegation of secret keys for different cipher text classes for different user and a single cipher text class index remains constant for same user in cloud storage. No matter which one among the power set of classes, the delegate can always get an aggregate key of constant size.

PROPOSED STRUCTURE

The data owner establishes the public system parameter through Setup and generates a public/master-secret key pair through KeyGen. Data can be encrypted via Encrypt by anyone who also decides what ciphertext class is associated with the plaintext message to be encrypted. Here data owner can encrypt and share multiple files using same constant cipher text class index towards to reduce the no of Class index files for individual files thus it improve the performance and storage space. The data owner can use the master-secret key pair to generate an aggregate decryption key for a set of ciphertext classes through Extract. The generated keys can be passed to delegates securely through secure e-mails or secure devices Finally, any user with an aggregate key can decrypt any ciphertext provided that the ciphertext's class is contained in the aggregate key via Decrypt. Key aggregate encryption schemes consist of five polynomial time algorithms as follows:

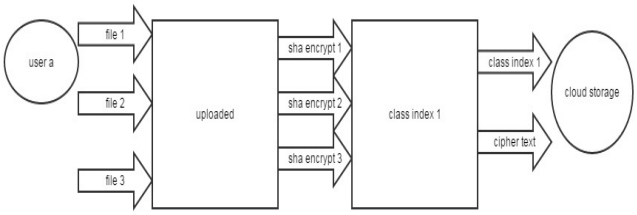

Fig 2. Proposed Architecture

1. SETUP (1λ , N) : The data owner establish public system parameter via Setup. On input of a security level parameter 1λ and number of ciphertext classes n , it outputs the public system parameter param

2. KEYGEN: It is executed by data owner to randomly generate a public/ master-secret key pair (Pk, msk).

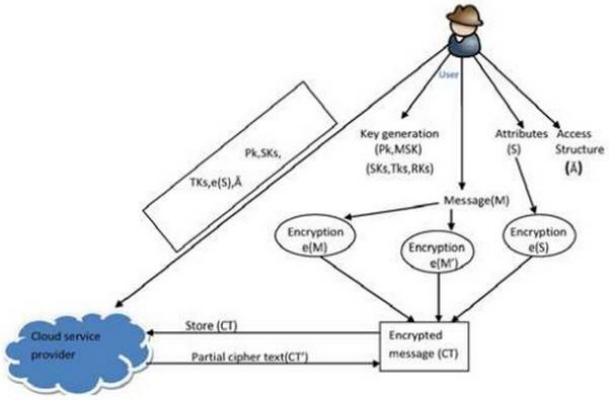

Fig 3. Key Generation Phase

3. ENCRYPT (PK, I, M) : It is executed by data owner and for message m and index i ,it computes the ciphertext as C.

For Encryption Advanced Encryption Standard AES is used , It is Symmetric algorithm with a block length of 128 bits. The key is arranged in the form of a matrix with 4 × 4 bytes. The key matrix is expanded into a schedule of 44 words. There are 10 rounds. For encryption, each round consists of the following four steps: 1) Substitute bytes, 2) Shift rows, 3) Mix columns, 4) Add round key Byte substitution (each value of the state is replaced with S-Box value) Shift rows (circular left shift on each row of the state) Mix columns (uses matrix multiplication in GF(256)) Add round key (bitwise XOR of current block with portion of expanded key) For decryption, each round consists of the following four steps: 1) Inverse shift rows, 2) Inverse substitute bytes, 3) Add round key, 4) Inverse mix columns.

4. EXTRACT (MSK, S): It is executed by data owner for delegating the decrypting power for a certain set of ciphertext classes and it outputs the aggregate key for set S denoted by Ks.

5. DECRYPT (KS, S, I, C): It is executed by a delegate who received, an aggregate key Ks generated by Extract. On input Ks, set S, an index i denoting the ciphertext class ciphertext C belongs to and output is decrypted result m

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 12, December 2015
Available at http://internationaljournalofresearch.org

DATA SHARING

KAC in meant for the data sharing. The data owner can share the data in desired amount with confidentiality. KCA is easy and secure way to transfer the delegation authority.

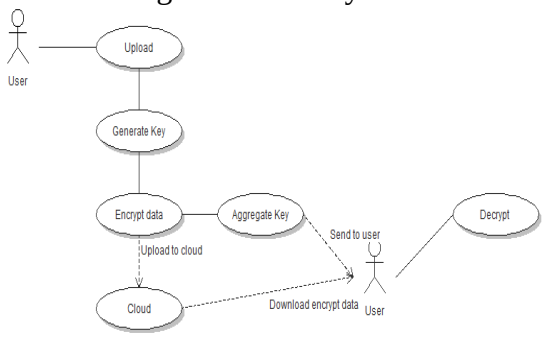

Fig 4. Use Case of Proposed System

For sharing selected data on the server Alice first performs the Setup. Later the public/master key pair (pk, mk) is generated by executing the KeyGen. The msk master key is kept secret and the public key pk and param are made public. Anyone can encrypt the data m and this data is uploaded on server. With the decrypting authority the other users can access those data. If Alice is wants to share a set S of her data with a friend Bob then she can perform the aggregate key KS for Bob by executing Extract (mk, S). As kS is a constant size key and the key can be shared through secure e-mail. When the aggregate key has got Bob can download the data and access it. 5.

String matching algorithms looks very simple and works very express than any other algorithms. Its computation cost is very low. it maintains the confidentiality, authentication and privacy factors in a finest way. The main advantage of using string matching algorithm is that it check one by one word for matching. So that a 100% recovery is done in a very simple way. This is the best way for confidential matching of strings.

PROPERTIES OF KAC

Decryption key size:- constant.
Cipher text size:- constant.
Encryption type:- public-key

5. CONCLUSION

To share data versatile is the essential thing in Cloud computing. Clients like to exchange their data on the cloud and among unmistakable customers. Outsourcing of data to the server may discharge the private data of a customer to everyone. Encryption is one arrangement which provides for bestowing pick data to fancied contender. Sharing of interpreting keys secure expects indispensable part. Open key cryptosystems give arrangement of mystery keys to unmistakable ciphertext classes in appropriated stockpiling. The agent gets securely a total key of predictable size. It is obliged to keep enough number of figure compositions classes as they manufacture snappy and the ciphertext classes are restricted that is the hindrance.

REFERENCES

[1] H.Fareesa Firdose , R.Deepthi Crestose Rebekah,"A Key Aggregate Construction with Adaptable Offering of Information in Cloud " INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS VOLUME 2, ISSUE 5, MAY 2015, PP 355-358 , ISSN (Online): 2349-7084. www.ijcert.org

[2] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, Privacy- Preserving Public Auditing for Secure Cloud Storage, IEEE Trans. Computers, vol. 62, no. 2, pp. 362–375, 2013.

[3] S.Kamara and K.Lauter,―Cryptographic Cloud Storage,Proc.Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010

[4] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, Aggregate and Verifiably Encrypted Signatures from Bilinear Maps, in Proceedings of Advances in Cryptology - EUROCRYPT '03, ser. LNCS, vol. 2656. Springer, 2003, pp. 416–432.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data, in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06). ACM, 2006, pp. 89–98.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing, Proc. IEEE INFOCOM, pp. 534-542, 2010.

[7] 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, 2009, pp. 121–130

[8] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 3, 2009.

[9] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," in Proceedings of ACM Workshop on Cloud Computing Security (CCSW '09). ACM, 2009, pp. 103–114.

[10] F. Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-Identity Single-Key Decryption without Random Oracles," in Proceedings of Information Security and Cryptology (Inscrypt '07), ser. LNCS, vol. 4990. Springer, 2007, pp. 384–398.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06). ACM, 2006, pp.89–98.