International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 3, March 2015
Available at http://internationaljournalofresearch.org

A Key Aggregate Framework with Adaptable Offering of Information in Cloud

[1]P.S.Sandhya Kumari ; [2]Dr. P. Venkateswarlu & [3]Md.Afzal

[1]M.Tech (CSE), Department of Computer Science & Engineering
Nagole Institute of Technology & Science, Kuntloor (V), Hayathnagar (M), RR District, Hyderabad, India.
E-mail id:sandhya0339@gmail.com
[2]Professor & HOD, Department of Computer Science & Engineering.
E-mail id: venkat123.pedakolmi@gmail.com
[3]Assistant Professor, Department of Computer Science & Engineering.
E-mail id: afzal.rubeena@gmail.com

Abstract-

In Cloud computing, data storage is an efficient technique. This investigation explains secure, efficient, and flexible method to share data with other people in cloud storage system. This survey, describe novel public-key cryptosystems. This system produce constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts are possible. This innovation scheme can aggregate any set of secret keys and make them as a compact single key .The power of all the keys being aggregated in a single key. In other words, holder of the secret key can release a constant-size aggregate key for flexible choices of cipher text set in cloud storage .In this scheme other encrypted files outside the cipher text set remain confidential. The compact aggregate key can be suitably sent to others or be stored in a smart card with very limited secure storage.

Keywords:

Aggregate key cryptosystem; Cloud storage; data sharing; key aggregate encryption.

1. INTRODUCTION

Cloud storage is nowadays very popular storage system. Cloud storage is storing of data off-site to the physical storage which is maintained by third party. Cloud storage is saving of digital data in logical pool and physical storage spans multiple servers which are manage by third party. Third party is responsible for keeping data available and accessible and physical environment should be protected and running at all time. Instead of storing data to the hard drive or any other local storage, we save data to remote storage which is accessible from anywhere and anytime. It reduces efforts of carrying physical storage to everywhere. By using cloud storage we can access information from any computer through internet which omitted limitation of accessing information from same computer where it is stored. While considering data privacy, we cannot rely on traditional technique of authentication, because unexpected privilege escalation will expose all data. Solution is to encrypt data before uploading to the server with user's own key. Data sharing is again important functionality of cloud storage, because user can share data from anywhere and anytime to anyone. For example, organization may grant permission to access part of sensitive data to their employees. But challenging task is that how to share encrypted data. Traditional way is user can download the encrypted data from storage, decrypt that data and send it to share with others, but it loses the importance of cloud storage. Cryptography technique can be applied in a two major ways- one is symmetric key encryption and other is asymmetric key encryption. In symmetric key encryption, same keys are used for encryption and

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

decryption. By contrast, in asymmetric key encryption different keys are used, public key for encryption and private key for decryption. Using asymmetric key encryption is more flexible for our approach. This can be illustrated by following example. Suppose Alice put all data on Box.com and she does not want to expose her data to everyone. Due to data leakage possibilities she does not trust on privacy mechanism provided by Box.com, so she encrypt all data before uploading to the server. If Bob ask her to share some data then Alice use share function of Box.com. But problem now is that how to share encrypted data. There are two severe ways: 1. Alice encrypt data with single secret key and share that secret key directly with the Bob. 2. Alice can encrypt data with distinct keys and send Bob corresponding keys to Bob via secure channel. In first approach, unwanted data also get expose to the Bob, which is inadequate. In second approach, no. of keys is as many as no. of shared files, which may be hundred or thousand as well as transferring these keys require secure channel and storage space which can be expensive. Therefore best solution to above problem is Alice encrypts data with distinct public keys, but send single decryption key of constant size to Bob. Since the decryption key should be sent via secure channel and kept secret small size is always enviable. To design an efficient public-key encryption scheme which supports flexible delegation in the sense that any subset of the ciphertexts

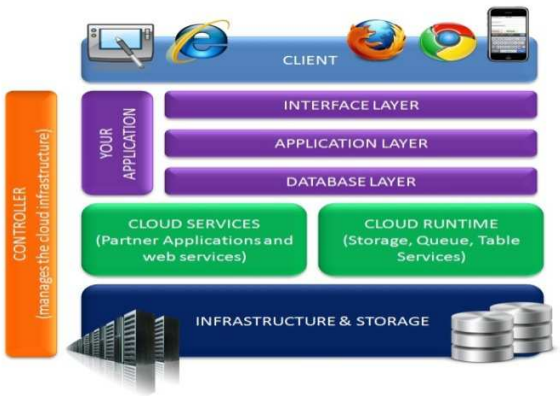

Fig 1 Cloud Computing Architecture

1.1 Cloud key characteristics

On-Demand Self-Service: Cloud client will build use of cloud resources with none human interaction between them and therefore the cloud service supplier (CSP).In addition; they'll schedule, manage and deploy any of cloud services like computation and storage once required. This results in reduction within the personnel overhead of the cloud supplier, cut in prices of the offered services.

Broad Network Access: Cloud services area unit accessible over the network via standardized interfaces that allows users to access the services not solely by advanced devices like personal computers, however conjointly by light-weight weight devices like sensible phones. Additionally, the lowered price of high-bandwidth network communication to the cloud provides access to a bigger pool of IT resources that sustain a high level of utilization.

Location-Independent Resource Pooling: The cloud should be ready to meet consumer's desires from resources. To do so, the cloud uses a method known as virtualization that allows the cloud supplier to pool his computing resources. This resource pool allows the sharing of virtual and physical resources by multiple shoppers. As declared by bureau, There could be a sense of location independence in this the client usually has no management or information over the precise location of the provided resources however could also be ready to specify location at a better level of abstraction.

Rapid Elasticity: it's the power of the cloud to assign and unleash resources quickly and expeditiously so as to satisfy the wants of the self-service characteristic of cloud computing. This machine-controlled method decreases the acquisition time for brand new computing capabilities once the requirement is there, whereas preventing associate abundance of unused computing power once the requirement has subsided. Measured Service: Cloud computing will dynamically and mechanically live the used resources by cloud customers. These measurements are often wont to bill the client and supply them with payment model supported pay-per-use. The bureau read of measured service is Cloud systems mechanically management and optimize resource use by investment a metering capability at some level of abstraction applicable to the kind of service

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

(e.g., storage, processing, bandwidth, and active user accounts). Resource usage are often monitored, controlled, and reportable providing transparency for each the supplier and client of the utilized service

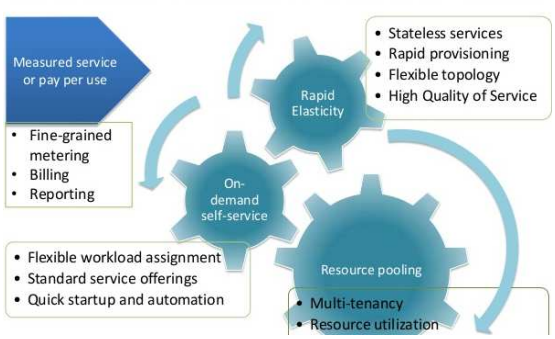

Fig 2 Cloud Computing Characteristics and Application

2. LITERATURE SURVEY

Cloud computing is visualized as architecture for succeeding generation. It has many facilities though have a risk of attacker who can access the data or leak the users identity. While setting a cloud users and service providers authentication is necessary. The issue arises whether loud service provider or user is not compromised. The data will leak if any one of them in compromised. The cloud should be simple, preserving the privacy and also maintaining users identity [1] The flexible use of cloud storage for user is a need as it is seams accessing data locally though that is present at remote side. It is important to inspect the data set on the cloud. So it is necessary to allow a public audit for integrity of outsourced data through third party auditor (TPA). TPA is also beneficial for cloud service provider. It checks the correctness of the outsourced data. TPA should be able to do public audit ability, storage correctness, privacy preserving, Batch auditing with minimum communication and computation overhead [2]. There are many cloud users who wants to upload there data without providing much personal details to other users. The anonymity of the user is to be preserved so that not to reveal the identity of data owner. Provable data possession (PDP) uses similar demonstrating marks to reduce computation on server, and network traffic. PDA ensures the data present on cloud which is un-trusted is original without accessing it. Security mediator (SEM) is approach allows the user to preserve the anonymity. Users are meant to upload all their data to SEM so that the SEM is not able to understand the data although it's going to generate the verification on data. As the users are signed at SEM it should not know the identity of uploader [3]. Another way for sharing encrypted data is Attribute-Based Encryption (ABE). It is likely to encrypt the data with attributes which are equivalent to users attribute rather than only encrypting each part of data. In ABE attributes description is considered as set so that only a particular key which is matched with attribute can decrypt the ciphertext. The user key and the attribute are matched if it matches it can decrypt a particular ciphertext. When there is k attributes are overlay among the ciphertext and a private key the decryption is granted [5]. A multi group key management accomplishes a hierarchical access control by applying an integrated key graph also handling the group keys for different users with multiple access authorities. Centralized key management plan uses tree structure to minimize the data processing, communication and storage overhead. It maintains things related to keying and also updates it. It accomplishes an integrated key graph for every user [6]. Identity-based encryption (IBE) is a vital primary thing of identity bases cryptography. The public key of user contains distinct information of user's identity. The key can be textual value or domain name, etc. IDE is used to deploy the public key infrastructure. The identity of the user is used as identity string for public key encryption. A trusted party called private key generator (PKG) in IBE which has the master secret key and gives secret key to users according to the user identity. The data owner collaborate the public value and the identity of user to encrypt the data. The ciphertext is decrypted using secret key [7]. In a multi attribute-authorities numbers of attributes are analyzed regarding the decryption key and the user must get a particular key related to the attribute while decrypting a message. The decryption keys are allocated independently to users those who have attribute identity without interaction between each other. Multi-authority attribute-based encryption allows real time deployment of attribute based

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

privileges as different attributes are issued by different authorities. The attribute authorities ensure the honesty of the user privilege so the confidentiality is maintained by central authority [8]. supply for cryptological keys

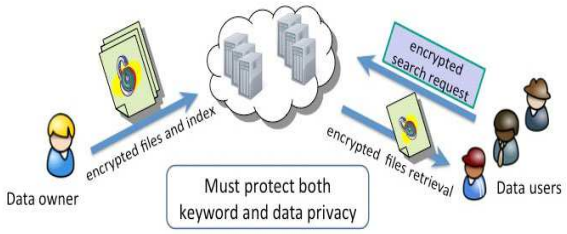

Fig 3 Secured data sharing architecture in cloud

3. RELATED WORK SYMMETRIC-KEY ENCRYPTION WITH COMPACT KEY

Benaloh et al. [2] presented an encryption scheme which is originally proposed for concisely transmitting large number of keys in broadcast scenario [3]. The construction is simple and we briefly review its key derivation process here for a concrete description of what are the desirable properties we want to achieve. The derivation of the key for a set of classes (which is a subset of all possible ciphertext classes) is as follows. A composite modulus is chosen where p and q are two large random primes. A master secret key is chosen at random. Each class is associated with a distinct prime. All these prime numbers can be put in the public system parameter. A constant-size key for set can be generated. For those who have been delegated the access rights for S' can be generated. However, it is designed for the symmetric-key setting instead. The content provider needs to get the corresponding secret keys to encrypt data, which is not suitable for many applications. Because method is used to generate a secret value rather than a pair of public/secret keys, it is unclear how to apply this idea for public-key encryption scheme. Finally, we note that there are schemes which try to reduce the key size for achieving authentication in symmetric-key encryption, e.g., [4]. However, sharing of decryption power is not a concern in these schemes.

IBE WITH COMPACT KEY

Identity-based encryption (IBE) (e.g., [5], [6], [7]) is a public-key encryption in which the public-key of a user can be set as an identity-string of the user (e.g., an email address, mobile number). There is a private key generator (PKG) in IBE which holds a master-secret key and issues a secret key to each user with respect to the user identity. The content provider can take the public parameter and a user identity to encrypt a message. The recipient can decrypt this ciphertext by his secret key. Guo et al. [8], [9] tried to build IBE with key aggregation. In their schemes, key aggregation is constrained in the sense that all keys to be aggregated must come from different ―identity divisions‖. While there are an exponential number of identities and thus secret keys, only a polynomial number of them can be aggregated.[1] This significantly increases the costs of storing and transmitting ciphertexts, which is impractical in many situations such as shared cloud storage. As Another way to do this is to apply hash function to the string denoting the class, and keep hashing repeatedly until a prime is obtained as the output of the hash function.[1] we mentioned, our schemes feature constant ciphertext size, and their security holds in the standard model. In fuzzy IBE [10], one single compact secret key can decrypt ciphertexts encrypted under many identities which are close in a certain metric space, but not for an arbitrary set of identities and therefore it does not match with our idea of key aggregation.

ATTRIBUTE-BASED ENCRYPTION

Attribute-based encryption (ABE) [11], [12] allows each ciphertext to be associated with an attribute, and the master-secret key holder can extract a secret key for a policy of these attributes so that a ciphertext can be decrypted by this key if its associated attribute conforms to the policy. For example, with the secret key for the policy (1 ∨ 3 ∨ 6 ∨ 8), one can decrypt ciphertext tagged with class 1, 3, 6 or 8. However, the major concern in ABE is collusion-resistance but not the compactness of secret keys. Indeed, the size of the key often increases linearly with the number of attributes it encompasses, or the ciphertext-size is not constant (e.g., [13]).

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

FRAMEWORK

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. 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:

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).

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

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.

4. 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. The aim of KCA is illustrated in Figure 4.

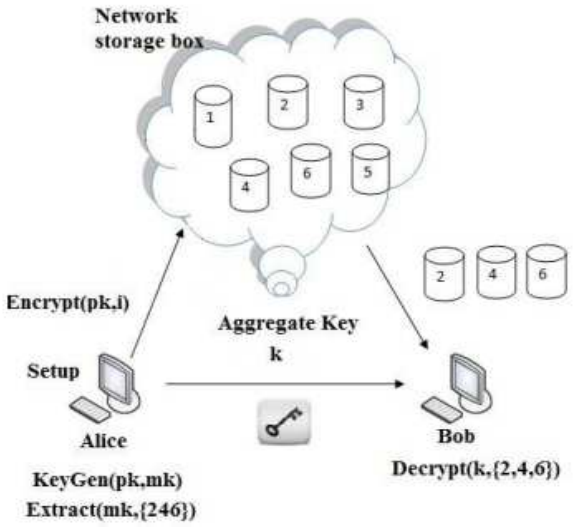

Fig 4. Use of KAC for data sharing

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.

5. CONCLUSION

To share data flexibly is vital thing in cloud computing. Users prefer to upload there data on cloud and among different users. Outsourcing of data to server may lead to leak the private data of user to everyone. Encryption is a one solution which provides to share selected data with desired candidate. Sharing of decryption keys in secure way plays important role. Public-key cryptosystems provides delegation of secret keys for different ciphertext classes in cloud storage. The delegatee gets securely an aggregate key of constant size. It is required to keep enough number of cipher texts classes as they increase fast and the ciphertext classes are bounded that is the limitation.

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

REFERENCES

[1] 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.

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

[3] 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.

[4] 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.

[5] 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.

[6] 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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

ABOUT THE AUTHOR

Ms.P.S.Sandhya, pursuing M.Tech (CSE) from Department of Computer Science & Engineering, "Nagole institute of technology & science", Hyderabad. India received B.Tech Degree in Computer Science & Engineering from Jawaharlal Nehru Technological University, Hyderabad in 2013.