Scientific Journal of Impact Factor(SJIF): 3.134

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 3, March -2015

Using Key-Aggregate Cryptosystem (KAC) Scheme Data Sharing In Cloud Storage

SandeepPatil[1], Ramesh Medar[2]

[1]Computer Science and Engineering, GIT college belgaum
[2]Computer Science and Engineering, GIT college belgaum

Abstract: *-Data sharing is an important function in cloud storage. Secure, efficient, and flexible sharing of data with others in cloud storage is studied. The public-key cryptosystems describes that any number of fixed-size cipher texts can be produced that helps in efficient assignment of decryption rights for any set of cipher text is possible. The innovative idea is that one can aggregate any set of secret keys and make them as compact as a single key, but covering the power of all the keys being aggregated. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of cipher text set in cloud storage, but the other encrypted files outside the set remain confidential. This compact aggregate key can be conveniently sent to others or be stored in a smart card with very limited secure storage.*

Keyword: *-Key size, master secret key, data security, data sharing, cloud storage, key-aggregate encryption.*

I. INTRODUCTION

Cloud Computing is a latest and fast growing technology that offers an innovative, efficient & scalable business model for organization to adapt various information technology resources i.e., software, hardware, storage, bandwidth etc.. Cloud computing has the capability to incorporate multiple internal and external cloud services together to provide high interoperability. There can be multiple accounts related with a single or multiple Service Provider (SP'_s). So Security is most important aspects in Cloud Computing Environment. The Cloud has become a new vehicle for delivering resources such as computing storage & sharing of data to customer in demand rather than being a new technology in itself, the Cloud is a new Business Model is enclosed around new Technologies such as server Virtualization that take advantage in Economics of scale and multi-tenancy to reduce the coust of using Information Technologies Resources

Cloud computing has evolved through a number of phases which include grid and utility computing, Application Service Provision (ASP), and Software as a Service (SaaS)**.**But the overarching concept of delivering computing resources through a global network is rooted in the sixties. Since the sixties, cloud computing has developed along a number of lines, with Web 2.0 being the most recent evolution. However, since the internet only started to offer significant bandwidth in the nineties, cloud computing for the masses has been something of a late developer.

One of the first milestones for cloud computing was the arrival of Salesforce.com in 1999, which pioneered the concept of delivering enterprise applications via a simple website. The services firm paved the way for both specialist and mainstream software firms to deliver applications over the internet. The next development was Amazon Web Services in 2002, which provided a suite of cloud based services including storage, computation and even human intelligence through the Amazon Mechanical Turk.

Then in 2006, Amazon launched its Elastic Compute Cloud (EC2) as a commercial web service that allows small companies and individuals to rent computers on which to run their own computer applications. “Amazon EC2/S3 was the first widely accessible cloud computing infrastructure service," said Jeremy Allier, CEO of Bright cove.

Another big milestone came in 2009, as Web 2.0 hit its stride, and Google and others started to offer browser-based enterprise applications, though services such as Google Apps. The most important contribution to cloud computing has been the emergence of "killer apps" from leading technology giants such as Microsoft and Google. When these companies deliver services in a way that is reliable and easy to consume, the knock-on effect to the industry as a whole is a wider general acceptance of online services," said Dan Germain, chief technology officer at IT service provider Cobweb Solutions.

Other key factors that have enabled cloud computing to evolve include the maturing of virtualization technology, the development of universal high-speed bandwidth, and universal software interoperability standards, said UK cloud computing pioneer Jamie Turner.

Cloud storage is gaining popularity recently. In enterprise settings, the rise in demand for data outsourcing, which assists in the strategic management of corporate data? It is also used as a core technology behind many online services for personal applications. Nowadays, it is easy to apply for free accounts for email, photo album; file sharing and/or remote access, with storage size more than 25 GB. Together with the current wireless technology, users can access almost all of their files and emails by a mobile phone in any corner of the world. Considering data privacy, a traditional way to ensure it is to rely on the server to enforce the access control after authentication, which means any unexpected privilege escalation will expose all data.

1.1 What is Cloud Computing?

The US Department of Commerce's National Institute of Standard and Technology defined Cloud Computing as:"a model for enabling convenient on demand network access to a shared pool of configurable computing resources. E.g.:- (Network, Servers, Storage & Applications) services, that can be swiftly provisioned and released with minimal management effort or services provider interaction".

In simple terms Cloud Computing is an Internet based modes of computing where the shared information, software & other devices upon demand. This enables the end user to access the Cloud Computing resources any time from any platforms such as Cell phones, Mobiles or Desktop.

1.2 What is Cloud Storage?

Cloud storage is a service where data is remotely maintained, managed & backed up. The service is available to user over a network, which is frequently the Internet; it allows the user to store files online so that the user can access them from any location via the Internet.

The provider Company makes them available to the user online by keeping the uploaded files on a peripheral server. This gives companies using Cloud storage services ease & convenience but can potentially be costly. Users should also be aware that backing up their data is still required when using Cloud storage service because recovering data from Cloud storage is much slower than local backup.

Cloud storage is gaining esteem recently. In venture settings, the rise in demand for data outsourcing, which assists in the tactical management of mutual data? It is also used as a core technology behind many online services for personal applications. Currently, it is easy to apply for free accounts for email, photo album; file sharing and/or isolated access, with storage size more than 25 GB.As one with the modern wireless technology, users can access about all of their files and emails by a mobile phone in any corner of the world. Considering data solitude, a traditional way to ensure it is to rely on the server to enforce the access control after certification, which means any unexpected solitude escalation will expose all data.

Some of the useful cloud storage services that are available are:

- Drop box
- Google Drive
- Microsoft SkyDrive

II. LITERATURE SURVEY

In this section survey related to Data sharing In Cloud Storage Using Key-Aggregate Cryptosystem (KAC) Schemeis carried out. In past enough work has been done for to Data sharing In Cloud Storage Using Key-Aggregate Cryptosystem (KAC) Scheme

2.1Cryptographic Keys for a Predefined Hierarchy:

Cryptographic key assignment schemes aim [2], to minimize the expense in storing and managing secret keys for general cryptographic use. Utilizing a tree formation, a key for a given branch can be used to derive the keys of its descendant nodes. Just granting the parent key implicitly grants all the keys of its descendant nodes.

More superior cryptographic key assignment schemes support access policy that can be modeled by an acyclic graph or a cyclic graph.

Drawbacks

Most of these schemes produce keys for symmetric-key cryptosystems, even though the key derivations may need modular arithmetic as used in public-key cryptosystems, which are generally more luxurious than "symmetric-key operations" such as pseudorandom function

2.2 Compact Key in Symmetric-Key Encryption:

An encryption scheme [3] which is originally proposed for concisely transmitting large number of keys in broadcast scenario.

2.3 Compact Key in Identity-Based Encryption (IBE):

IBE [4][5]is a type of public-key encryption in which the public-key of a user can be set as an identity string of the user. There is a trust party called as private key generator in IBE which holds a master-secret key and issues a secret key to each user with respect to the user identity. The encryptor can get the public parameter and a user identity to encrypt a message. The recipient can decrypt this cipher text by his secret key.

2.4Attribute-based encryption (ABE)**:**

ABE [6] allows each cipher text to be associated with an characteristic, and the master-secret key holder can extract a secret key for a policy of these attributes so that a cipher text can be decrypted by this key if its associated attribute conforms to the policy.

2.5 Primitive is proxy re-encryption (PRE):

To delegate the decryption power of some cipher texts without sending the secret key to give, a useful primitive is proxy re-encryption (PRE)[7]. A PRE scheme allows sender to delegate to the server (proxy) the ability to convert the cipher texts encrypted under her public-key into ones for receiver

III. PROBLEM STATEMENT

The proposed system problem statement is "To design adaptable and efficacious public-key encryption that will delegate any subset of cipher texts (produced by encryption scheme) and is decrypt able by a fixed-size decryption key."

Therefore, the above design is a special type of public-key encryption which we call Key-Aggregate Cryptography (KAC).

IV. PROPOSED SYSTEM

- To study how to make a decryption key more powerful in the sense that it allows decryption of numerous cipher texts, without increase in size.
- To design an efficient public-key encryption scheme which supports flexible delegation in the sense that any subset of the cipher texts is decrypt able by a constant-size decryption key?
- To introduce a special type of public-key encryption which called as key-aggregate cryptosystem (KAC).
- In KAC, users encrypt a message not only under a identifier, but also under an public-key of ciphertext called class.
- That means the ciphertexts are more categorized into different classes. The key vendor holds a master-secret called master-secret key, which can be used to take secret keys for different classes.

- Moreover, the extracted key have can be an aggregate key which is as compact as a secret key for a distinct class, but aggregates the authority of many such keys, i.e., the decryption authority for any subset of ciphertext classes.
- Aggregate key can be sent to receiver via a secure e-mail.
- Receiver can download the encrypted content and then use this aggregate key to decrypt these encrypted photos.

V. SYSTEM DESIGN (SYSTEM ARCHITECTURE)

A software product is a complex unit. Its development usually follows what is known as Software Development Life Cycle (SDLC). The second stage in the SDLC is the Design stage. The impartial of the design stage is to produce the overall design of the software.

The following design illustrates the proposed model of KAC Scheme:

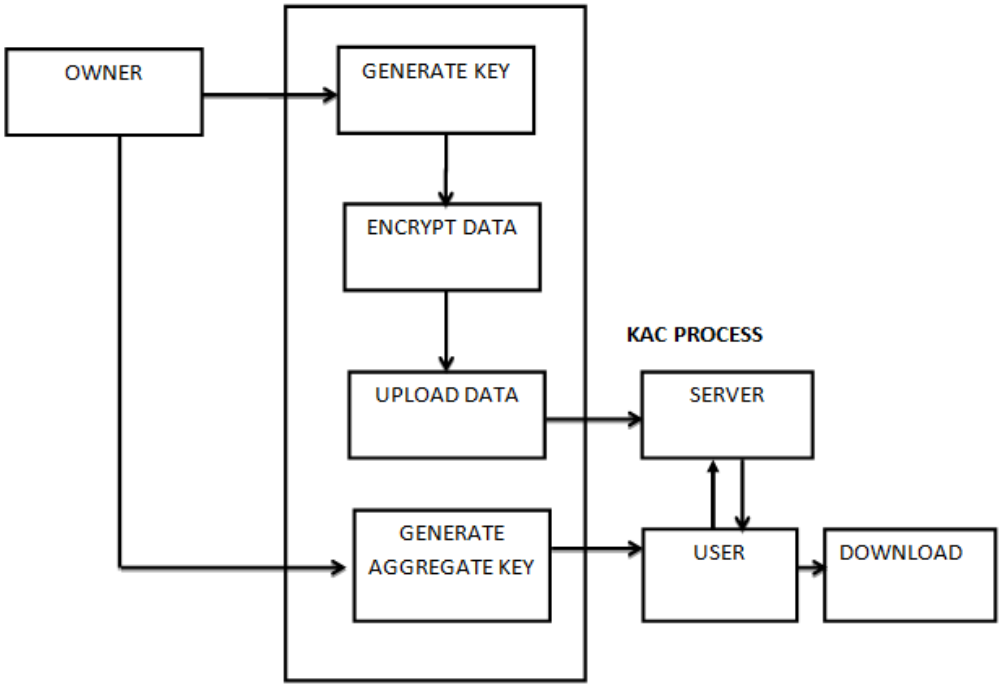

Figure 5.1System Architecture of KAC Scheme

VI. NECESSITY OF THE PROPOSED SYSTEM

The above stated problem definition, suggests that the proposed system is necessary for the following reasons:

- This scheme provides high security to the data that is stored in cloud while sharing.
- In the other existing schemes of cryptography, it is observed that multiple encryption and decryption functions are not supported. In the proposed system, it allows decryption of multiple ciphertexts, without increasing the key size.
- The keys required for decrypting the multiple ciphertexts are aggregated into a class for decryption. This aggregation of keys into a class doesn't increase the size.

- This is also necessary so as to provide less overhead in key storage.

VII. SUMMARY

In this paper, we have considered and tried to resolve an important question of how to protect user's data privacy on cloud storage. The "compression" of secret keys in public- key cryptosystems is discussed which also supports delegation of Secret keys for different cipher text classes in clouds storage. This approach more flexible as it saves spaces. An important feature of this approach is that the designate (receiver) can always get an aggregate key of constant size.

REFERENCE

[1] Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, Senior Member, IEEE "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014

[2] G. Ateniese, A.D. Santis, A.L. Ferrara, and B. Masucci, "Provably-Secure Time-Bound Hierarchical Key Assignment Schemes,"J. Cryptology, vol. 25, no. 2, pp. 243-270, 2012.

[3] J. Benaloh, "Key Compression and Its Application to Digital Fingerprinting," technical report, Microsoft Research, 2009.

[4] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '05), vol. 3494, pp. 457-473, 2005.

[5] S.S.M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, "Practical Leakage-Resilient Identity-Based Encryption from Simple As-sumptions," Proc. ACM Conf. Computer and Comm. Security, pp. 152-161, 2010

[6] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security,pp. 121-130. 2009,

[7] C.-K. Chu, J. Weng, S.S.M. Chow, J. Zhou, and R.H. Deng, "Conditional Proxy Broadcast Re-Encryption,"Proc. 14th Austra-lasian Conf. Information Security and Privacy (ACISP '09), vol. 5594, pp. 327-342, 2009

