International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)

http://www.ijcsjournal.com Volume 3, Issue 2, No 1, 2015. ISSN: 2348-6600
Reference ID: IJCS-098 PAGE NO: 561-567.

SCALABLE KEY AGGREGATION OF CRYPTOSYSTEM FOR DATA SHARING IN CLOUD STORAGE

Miss. Syed.shaheen, (M.Tech Student),
Department of Computer Science and technology
Madina Engineering College,
Andhra Pradesh, Kadapa, India.
Syedshahin_13@gmail.com

Sri. K. Sreenivasulu, Professor&H.O.D,
Department of Computer Science and technology
Madina Engineering College,
Andhra Pradesh, Kadapa, India.
sreenu.kutala@gmail.com

Abstract*— *A scalable data sharing is a crucial functionality in cloud storage. In this paper we deploy efficient and flexible, privacy share data communication in cloud storage. By the privacy consideration we deploy a public-key cryptosystems that produce constant-size cipher texts such that efficient delegation of decryption rights for all sets of cipher-texts is possible. The granularity is that one can combined all set of secret keys and make it as single key, but encompassing the power of all keys being aggregated that is the secret key holder can release a context-size aggregate key for flexible choice of cipher-text set in cloud storage and remaining encrypted files are confidential. This compact aggregate key can be sent to others as a convenient manner or it stored a limited size of secure data in smart card. We describe a casual security analysis of our schemas in standard model with an application of schemas along with public-key patient controlled encryption (PCE) for flexible hierarchy it has to be known

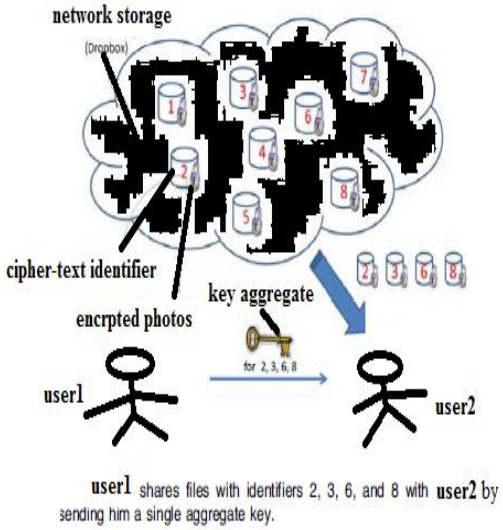
Index Terms: Cloud storage, Data sharing, KAE, and PCE.

I.INTRODUCTION

Most of the cloud storages are used for data storage purpose Cloud storage is gaining popularity recently. Generally cloud is a Meta data of internet cloud computing. Cloud computing is the long dreamed vision ofcomputing as a utility, where cloud customers canremotely store their data into the cloud so as to enjoy theon-demand high-quality applications and services from a shared pool of configurable computing resources great flexibility and economic savings are motivating both individuals and enterprises to outsource their local complex data management system into the cloud. In enterprise settings, we see 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, and 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. In a shared-tenancy cloud computing environment, things become even worse. Data from different clients can be hosted on separate virtual machines (VMs) but reside on a single physical machine. Data in a target VM could be stolen by

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 2, No 1, 2015. ISSN: 2348-6600
Reference ID: IJCS-098 PAGE NO: 561-567.

instantiating another VM co- resident with the target one.A cryptographic solution, for example, with proven security relied on number-theoretic assumptions is more desirable, whenever the user is not perfectly happy with trusting the security of the VM or the honesty of the technical staff. These users are motivated to encrypt their data with their own keys before uploading them to the server.



user1 shares files with identifiers 2, 3, 6, and 8 with user2 by sending him a single aggregate key.

By the privacy consideration we deploy a public-key cryptosystems that produce constant-size cipher texts such that efficient delegation of decryption rights for all sets of cipher-texts is possible. The granularity is that one can combined all set of secret keys and make it as single key, but encompassing the power of all keys being aggregated that is the secret key holder can release a context-size aggregate key for flexible choice of cipher-text set in cloud storage and remaining encrypted files are confidential. This compact aggregate key can be sent to others as a convenient manner or it stored a limited size of secure data in smart card. We describe a casual security analysis of our schemas in standard model with a application of schemas along with public-key patient controlled encryption (PCE) for flexible hierarchy it has to be known.

1. CLOUD STORAGE:

Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data. Cloud storage services may be accessed through a co-located cloud computer service, a web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web -based content management systems .Cloud storage is based on highly virtualized infrastructure and is like broader cloud computing in terms of accessible interfaces, near-instant elasticity and

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 2, No 1, 2015. ISSN: 2348-6600
Reference ID: IJCS-098 PAGE NO: 561-567.

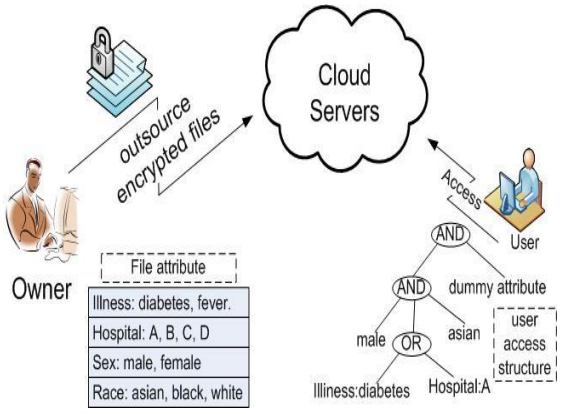
scalability, multi-tenancy, and metered resources. Cloud storage services can be utilized from an off-premises service or deployed on-premises Cloud storage typically refers to a hosted object storage service, but the term has broadened to include other types of data storage that are now available as a service, like block storage. Object storage services like Amazon S3 and Microsoft Azure Storage, object storage software like Open stack Swift , object storage systems like EMC Atoms and Hitachi Content Platform , and distributed storage research projects like Oceans tore and VISION Cloud are all examples of storage that can be hosted and deployed with cloud storage characteristics.

Cloud storage :

Made up of many distributed resources, but still acts as one - often referred to as federated storage clouds. Highly fault tolerant through redundancy and distribution of data highly durable through the creation of versioned copies. Typically eventually consistent with regard to data replicas

2. DATA SHARING:

Various sensitive data pooled in the cloud demands the cloud data sharing service to be responsible for secure, efficient and reliable enforcement of data content access among potentially large number of users on behalf of data owners. As cloud server may no longer be in the same trusted domain as the data owners, we have to rethink the problem of access control in this open environment, where cloud server takes full charge of the management of the outsourced data but are not necessarily trusted with respect to the data confidentiality. What makes the problem more challenging is the enforcement of fine-grained data access, the support of access privilege updates in dynamic scenarios, and the system scalability, while maintaining low level complexity of key management and data encryption. Our goal is to provide tools extending owners' full control over cloud data access and enabling all owners/users to benefit well from current capabilities of the cloud, so as to achieve finer, stronger, and more usable secure cloud data sharing services.To achieve fine-graininess, we propose to treat data as files associated with a set of meaningful attributes, use logical composition of attributes to reflect fine-grained data access, and enforce owner's control via attribute-based encryption.



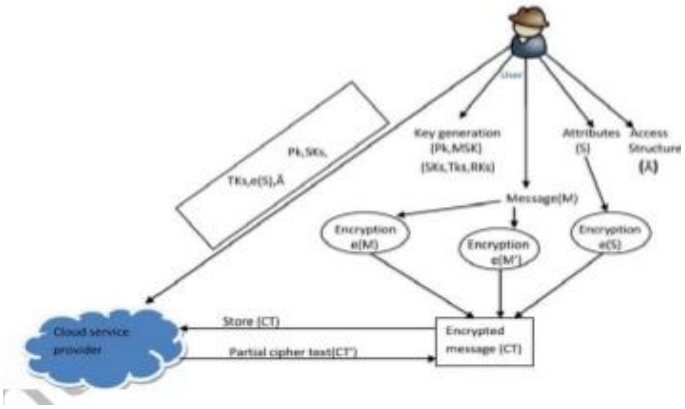
For the inherent scalability requirement of cloud system, where user access privilege updates happen very frequently and thus inevitably incurs significant user/data management burden on data owner, we further propose to treat the cloud as a mediated proxy, to which data owners can delegate most cumbersome workload, like handling user access privilege dynamics in large system, without affecting the underlying data confidentiality. In addition, we are also exploring other security goals in a practical cloud data sharing system, including user access privilege confidentiality, and user accountability in case of user access key abuse attacks.

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 2, No 1, 2015. ISSN: 2348-6600
Reference ID: IJCS-098 PAGE NO: 561-567.

3. KAE:

An aggregate signature scheme is a digital signature that supports aggregation: Given *n* signatures on *n* distinct messages from *n* distinct users, it is possible to aggregate all these signatures into a single short signature. This single signature (and the *n* original messages) will convince the verifier that the *n* users did indeed sign the *n* original messages (i.e., user *i* signed message M_i for $i = 1,...,n$). In this paper we introduce the concept of an aggregate signature, present security models for such signatures, and give several applications for aggregate signatures. We construct an efficient aggregate signature from a recent short signature scheme Aggregate signatures are useful for reducing the size of certificate chains (by aggregating all signatures in the chain) and for reducing message size. A key-aggregate encryption scheme consists of five polynomial-time algorithms as follows. The data owner establishes the public system parameter via Setup and generates a public/master-secret3 key pair via Key-Gen. Messages can be encrypted via Encrypt by anyone who also decides what cipher-text class is associated with the plaintext message to be encrypted. The data owner can use the master-secret to generate an aggregate decryption key for a set of cipher-text classes via Extract. The generated keys can be passed to delegates securely (via secure e-mails or secure devices) finally; any user with an aggregate key can decrypt any cipher-text provided that the cipher-ext class is contained in the aggregate key via Decrypt.



ALGORITHM:

Setup (1, n): executed by the data owner to setup an account on an un-trusted server. On input a security level parameter 1 and the number of cipher-text classes n (i.e., class index should be an integer= bounded by 1 and n), it outputs the public system parameter param, which is omitted from the input of the other algorithms for brevity.

Key-Gen: executed by the data owner to randomly generate a public/master-secret key pair (pk,msk).

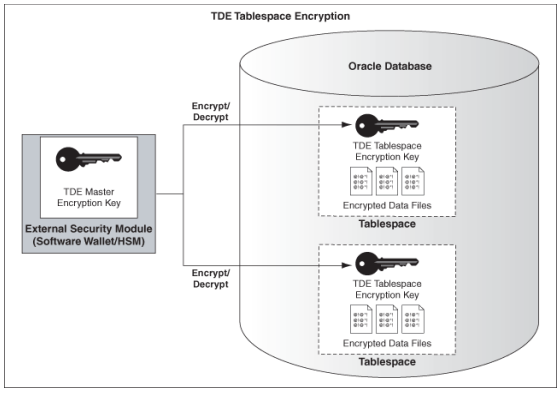
Encrypt (pk, I,m): executed by anyone who wants to encrypt data. On input a public-key pk, an index i denoting the ciphertext class, and a message m, it outputs a cipher-text C.

Extract (msk, S): executed by the data owner for delegating the decrypting power for a certain set of cipher-text classes to a delegatee. On input the master-secret key msk and a set S of indices corresponding to different classes, it outputs the aggregate key for set S denoted by KS.

Decrypt (KS, S, I, C): executed by a delegatee who received an aggregate key KS generated by Extract.

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 2, No 1, 2015. ISSN: 2348-6600
Reference ID: IJCS-098 PAGE NO: 561-567.

Transparent Data Encryption (TDE) column encryption enables you to encrypt sensitive data stored in select table columns. TDE table space encryption enables you to encrypt all data stored in a table space. Both TDE column encryption and TDE table space encryption use a two-tiered, key-based architecture. Even if the encrypted data is retrieved, it cannot be understood until authorized decryption occurs, which is automatic for users authorized to access the table.



CRYPTOGRAPHIC SYSTEMS IN KEY ENCRPTION:

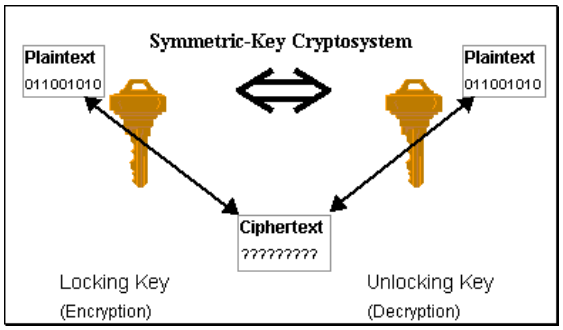
Historically cryptographic systems have provided only confidentiality. Preparing a message for a secure, private transfer involves the process of encryption. Encryption transforms data in user or machine readable form, called the plaintext, to an illegible version, called the cipher-text. The conversion of plaintext to cipher-text is controlled by an electronic key *k*. The key is simply a binary string which determines the effect of the encryption function. The reverse process of transforming the cipher-text back into plaintext is called decryption, and is controlled by a related key *l*.

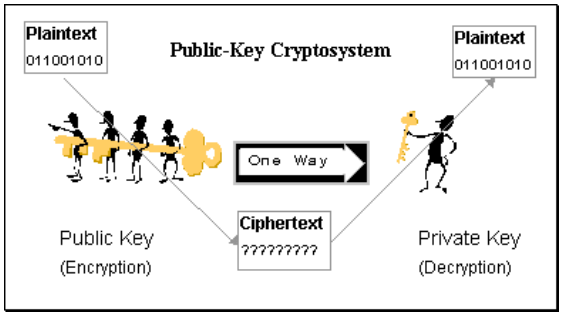
There are two broad classes of cryptosystems, known as symmetric-key cryptosystems and public-key cryptosystems. The relationship between *k*and *l* differentiates the two

In a symmetric-key cryptosystem, the same key is used for both encryption and decryption. Illustrates the mechanical analogy of a symmetric-key cryptosystem. Since the keys are the same, two users wishing to communicate in confidence must agree and maintain a common secret key. Each entity must trust the other not to divulge the key. In applications where a limited number of users exist, symmetric-key cryptography is effective. However, in large networks with users distributed over a wide area, key distribution becomes a problem. Each individual in a network should have a distinct key to communicate with each other person. To set this up, a tremendous number of keys must be established and stored securely. For example, a system with 1000 users would require approximately 500,000 keys to be exchanged and maintained securely. Exchanging and managing such a large number of keys is at best an arduous task and at worst impossible.

Symmetric-key cryptosystems have been used to provide confidentiality for thousands of years. One of the first recorded systems was used by Julius Caesar. Known as the Caesar Cipher, it involves shifting the letters of the alphabet a predetermined number of characters. The number of character shifts is the encryption key, and, of course, shifting back the same number of characters reverses this process to decrypt. Today, symmetric-key cryptosystems are controlled by keys that are based on complex mathematical algorithms.

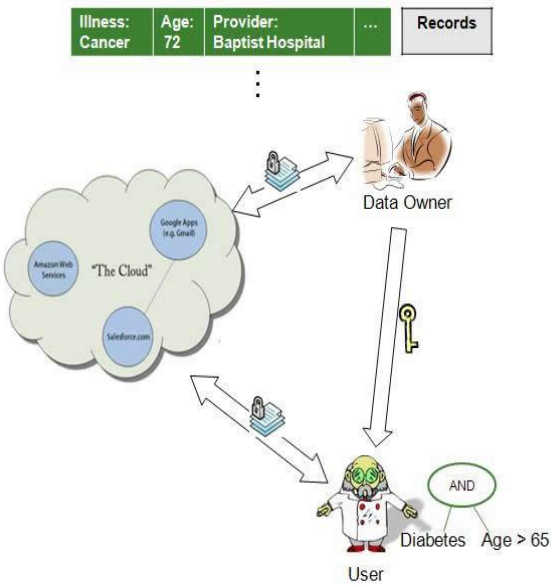
International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 2, No 1, 2015. ISSN: 2348-6600
Reference ID: IJCS-098 PAGE NO: 561-567.





4. PATIENT CONTROLLED ENCRYPTION (PCE):

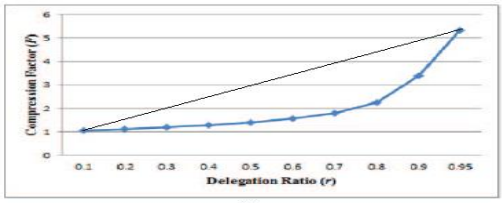
Moving into cloud introduces a challenging issue of securing data storage and sharing. Due to the open nature of the cloud, cloud customers may want to keep sensitive data confidential against cloud servers while storing them in the cloud. This requirement, however, would render flexible data sharing difficult since it rules out most traditional access control mechanisms in which the servers usually need to access data content. While data encryption provides a nature solution to data confidentiality, it also raises the tension between efficient key management and fine-grained data access control in large-scale applications. Our goal for this project is to solve this tension and allow cloud customers to enforce fine-grained access policies with scalability and efficiency.



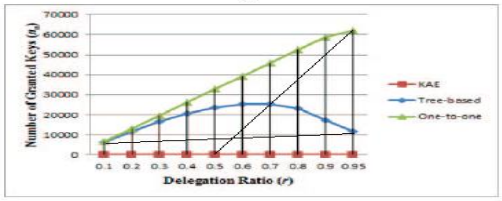
In this we propose to let cloud customers (data owners) encrypt data before outsourcing. We utilize attribute-based encryption for data encryption, in which attributes are defined for data and user decryption keys are associated with flexible access structures defined over the attributes. We allow cloud costumers to offload computation-intensive operations to cloud servers without disclosing data content. We achieve this with our novel computation delegation technique which uniquely combines attribute-based encryption with proxy re-encryption. In addition, our solution is able to provide user accountability and privacy preservation of access policies.

International Journal of Computer Science
ISSN:2348-6600
Oddity...Probe...Reviste...
Published by SK Research Group of Companies(SKRGC)
http://www.ijcsjournal.com Volume 3, Issue 2, No 1, 2015. ISSN: 2348-6600
Reference ID: IJCS-098 PAGE NO: 561-567.

RESULT ANALYSIS:



(a)



(b)

CONCLUSION:

How to 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 article, we consider how to "compress" secret keys in public-key cryptosystems which support delegation of secret keys for different cipher-text classes in cloud storage. No matter which one among the power set of classes, the delegate can always get an aggregate key of constant size. Our approach is more flexible than hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges.

FUTURE ENHANCEMENT:

A limitation in our work is the predefined bound of the number of maximum cipher-text classes. In cloud storage, the number of cipher-texts usually grows rapidly. So we have to reserve enough cipher-text classes for the future extension.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. On the other hand, when one carries the delegated keys around in a mobile device without using special trusted hardware, the key is prompt to leakage, designing a leakage-resilient cryptosystem yet allows efficient and flexible key delegation is also an interesting direction.