Secure Role base Access Control data Sharing Approach in Cloud Environment

Sneha Waikar, Chinmay Jain, Pranali Rananaware, Simran Bajaj, S. P. Pimpalkar
AISSMS Institute of Information Technology Kennedy Road, Near R.T.O., Pune 411 001

Abstract: With the popularity of cloud computing, mobile devices can store/retrieve personal data from anywhere at any time. Consequently, the data security problem in mobile cloud becomes more and more severe and prevents further development of mobile cloud. There are substantial studies that have been conducted to improve the cloud security. However, most of them are not applicable for mobile cloud since mobile devices only have limited computing resources and power. Solutions with low computational overhead are in great need for mobile cloud applications. In this paper, we propose a lightweight data sharing scheme (LDSS) for mobile cloud computing. It adopts CP-ABE, an access control technology used in normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud environments. LDSS moves a large portion of the computational intensive access control tree transformation in CP-ABE from mobile devices to external proxy servers. Furthermore, to reduce the user revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a thorny issue in program based CP-ABE systems. The experimental results show that LDSS can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments.

Keywords: RBAC, Cloud Computing, Data Security, Revocation

Introduction

Cloud Computing

Cloud computing is a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers. It relies on sharing of resources to achieve coherence and economy of scale, similar to a utility (like the electricity grid) over a network

IaaS

Infrastructure as a Service (IaaS) is a form of cloud computing that provides virtualized computing resources over the Internet. IaaS is one of three main categories of cloud computing services, alongside Software as a Service (SaaS) and Platform as a Service (PaaS).

Forward Security

In cryptography, forward secrecy (FS; also known as perfect forward secrecy) is a property of secure communication protocols in which compromise of long-term keys does not compromise past session keys. Forward secrecy protects past sessions against future compromises of secret keys or passwords. If forward secrecy is used, encrypted communications and sessions recorded in the past cannot be retrieved and decrypted should long-term secret keys or passwords be compromised in the future, even if the adversary actively interfered.

Cloud Utility Function

Utility computing, or The Computer Utility, is a service provisioning model in which a service provider makes computing resources and infrastructure management available to the customer as needed, and charges them for specific usage rather than a flat rate. Like other types of on-demand computing (such as grid computing), the utility model seeks to maximize the efficient use of resources and/or minimize associated costs. Utility is the packaging of computing resources, such as computation, storage and services, as a metered service. This model has the advantage of a low or no initial cost to acquire computer resources; instead, computational resources are essentially rented.

Introduction

Forward secure character based ring mark for information partaking in the cloud give secure information sharing of inside of the gathering in a productive way. It additionally give of the legitimacy and namelessness of the clients. Ring mark is the promising possibility to build an unknown and credible information sharing framework. It permits an information proprietor to thein mystery validate his information which can be put into the cloud for capacity or investigation reason. The framework can be to keep away from exorbitant testament check in the customary open key framework setting turns into a bottleneck for this answer for be versatile. Personality based ring the mark which is dispenses with of the procedure of testament for confirmation can be utilized. The security of the ID-based providing so as to ring mark as a forward security- If a mystery key of any client has been upheaval, then all past created marks that incorporate that client still stay legitimate. The property is particularly vital to any extensive size of information sharing framework, as it is difficult to ask all information proprietors to re-confirm their information regardless of the possibility that a mystery key of the one single client has been surrendered. Responsibility what's more, security issues with respect to cloud are turning into the noteworthy obstruction to the wide selection of cloud administrations. There is the part of headway happens in the framework concerning the web as a noteworthy worry in it'simplementation in a well compelling way separately furthermore give of the framework in multi-cloud environment. Huge numbers of the clients are a getting pulled in to this innovation because of the administrations included in it the took after by the diminished calculation took after by the expense furthermore the solid information of transmission happens in the framework in a well viable way respectively.[9]

Literature Survey

Existing examination work is accessible in the parts of uprightness confirmation of outsourced information, data stockpiling security on untrusted remote servers and access control of outsourced data. The word cloud had come to make reference to extensive Asynchronous Transfer Mode frameworks. By 21st century, he term "disseminated registering" had showed up, yet key fixate at this moment was on Software as a Service (SaaS). In 1999, bargains force.com was made by Parker Harris, Marc Benioff. They used various headways of client locales, for example, Yahoo and Google! to association programs. They furthermore gave the thoughts like" On hobby" and" SaaS" with their bona fide association and customers that were compelling. Cloud data stockpiling (Storage as a Service) is an essential organization of dispersed figuring insinuated as Infrastructure as a Service (IaaS). Amazon's Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3) are comprehended occurrences of cloud data stockpiling. On the other side close by these preferences' appropriated figuring defies tremendous test i.e. data stockpiling security issue, which is a basic part of Quality of Service (QoS). At the point when customer puts information on the cloud as opposed to locally, he has no impact over it i.e. unapproved customers could change customer's information or ruin it and even cloud server scheme ambushes. Cloud customers are generally struggled with steadiness and the security of the information in the cloud. Amazon's S3 [8] is such a fair case.

In paper [1], Identity based cryptosystem, presented by Shamir [1], disposed of the requirement for confirming legitimacy of open key endorsements, administration of both time and cost expending. In an ID based cryptosystem, general key of each client is effectively processable from string relating to this present client's openly known personality (e.g., a private location, an email address, and so on.). A private key generator (PKG), figures private keys from its expert mystery for all clients. This property maintains a strategic distance from the need of testaments and partners a verifiable open key (client personality) to every client inside of the framework. With a specific end goal to confirm an ID-based signature, unique in relation to the conventional for signature of open key based, one does not have to check endorsement first. And the end of authentication approval makes an entire confirmation handle more proficient, which will lead to significant recovery in correspondence and calculation at the point when countless are included (say, vitality utilization information partaking in brilliant matrix).

In paper [2], the prime appearance of ring mark in 1994 and the official presentation in 2001.Ring mark is utilized (Actual personality of endorser is covered up) in this paper. Ring mark is a gathering focused mark with security assurance on mark maker. In this paper we formalize the thought of a

ring mark, which makes it conceivable to determine an arrangement of conceivable underwriters without uncovering which part really created the mark. Dissimilar to gathering marks, ring marks have no gathering chiefs, no repudiation techniques, no setup systems, and no synchronization- any client can pick any arrangement of conceivable underwriters that incorporates himself, and sign any of the messages by using his mystery key and others open keys, without taking their help.

In paper [3], In this paper, We first upgrade their indicating in order to ring mark perspective that it holds under a totally weaker assumption, specifically the unpredictable prophet show rather than the ideal figure. By then utilize extensions to make ring marks suitable in practical circumstances, for instance, edge arranges or uncommonly delegated social occasions.

In paper [4], in this paper, we show another however culminate model whose security level can be thought to be lying amidst for the most part used models. Fine-grained refinements on the security models is basic to make following a couple arrangements may be secure in a portion of the models however not in the others.

In paper [5], in this paper Identity based ring mark was secure in self-assertive prophet model.

In paper [6], in this paper first Identity based ring mark expressed to be secure in the standard model is a result of this paper under the trusted setup supposition. However their affirmation isn't correct and is pointed out by [9]

In paper [7], in this paper, we formalize the definition and security considerations for a forward-secure character based imprint arrangement, and after that add to a capable arrangement. All parameters that are accessible in our arrangement have, at most, log-squared multifaceted nature to the extent the total number of time periods. Without subjective prophets the arrangement is provably secure..

Problem Statement

There are few concerns involving because the information owner physically releases sensitive information to some distant CSP:

• Confidentiality - Outsourced information has to be protected from users which are not allowed access, the CSP, and the TTP.
• Integrity - Outsourced data must keep undamaged on cloud servers. Authorized users and the information owner should be empowered to recognize information corruption.
• Access control – Authorized users only have to be permitted to gain access to the information that was outsourced.
• The defense of CSP - The CSP has to be safeguarded against fake accusations that could be stated by owner/users
that were dishonest, and this type of malicious conduct is needed to be disclosed.

Contributions

- Generate a real time disk failure problem, and recover whole data from VM with the help of Generated Matrix.
- Provide Role Base Access Control (RBAC) for user management.
- Proxy key generation when user revocation has occur by data owner.
- Execute the system with IAAS multi cloud environment.

PROPOSED SYSTEM

System Architecture

Forward secure identity predicated ring signature for data sharing in the cloud architecture that proposed data sharing in an efficient manner. This architecture, provide multiple cloud environment for astronomically immense data sharing in secure way. Client in the diagram represents individual cloud accommodation utilizer. The servers may exist in different physical locations. The CSP takes decision of the servers to store the data depending upon available spaces. Identity predicated ring signature provide the ring formation of users. The authentic data sharing in multiple clouds to provide secure data sharing at sizably voluminous system. The encryption and decryption provide secure data transmission.

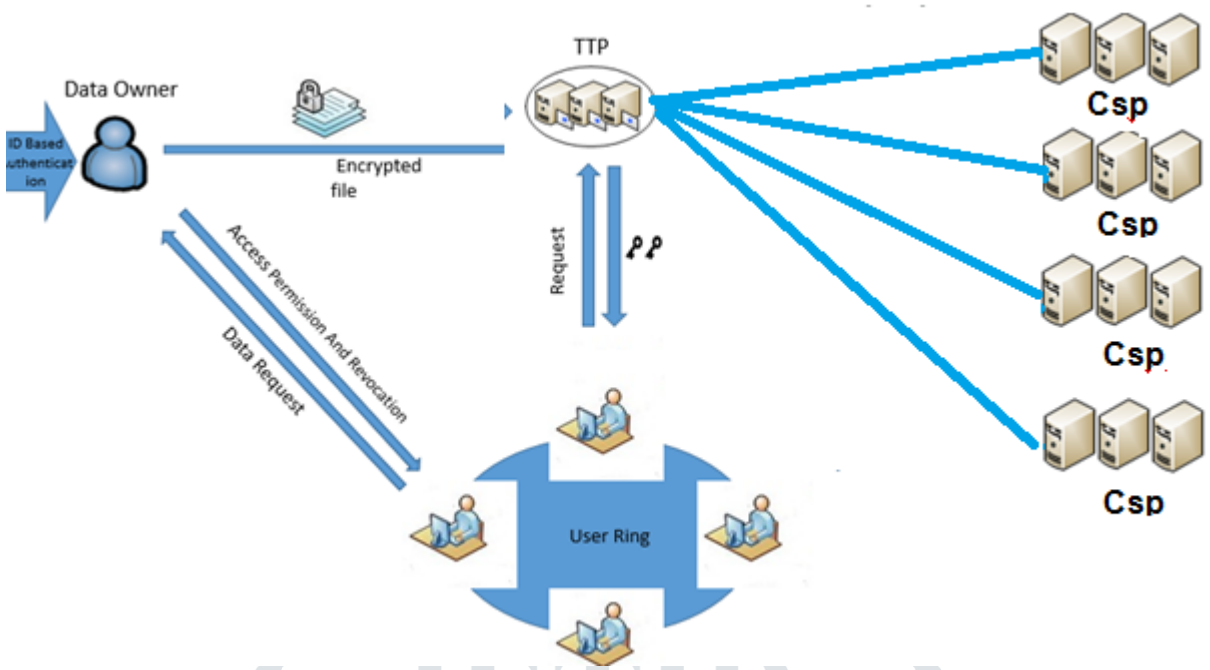

Figure 1: Proposed System Architecture

Data Owner

Information Owner of the device component is the nothing the user of desire to save and share data over cloud. Information owner isn't having any idea where my information will be stored by the CSP and there is trust shortfall on CSP.

As data is most important for info owner and the data owner do not desire that his information is observable to the CSP. To fix the preceding issue set trustworthy third party and before uploading the data, it's encrypted / auditor which are set to keep watch.

Trusted Third Party / Auditor

Database reviewing includes a database to not be uninformed of the activities of the database clients. Database heads and advisors every now and again set up evaluating for the security purposes. For instance to guarantee that exhortation to be gotten to by those without the consent don't get to it. Reviewing is the observing and recording of client database exercises that are chosen. It may be founded on blends of variables that can incorporate client name, system, time, etc, including the sort of SQL articulation executed, or on individual exercises. Reviewing can be activated by security approaches when indicated parts including, inside of an Oracle database are acquired or modified the substance inside of a given article.

For instance, the database executive can gather information about which tables are being redesigned, what number of coherent I/Os are performed, or what number of simultaneous clients unite at top times. Find issues with an authorization or access control execution

Authorized User

A client who has right to access the remote data is a Authorized User.

Cloud Storage Service Provider (CSP)

Database is provided by cloud Storage Services Provider. It permits information owner to keep any kind of information and also able to make the user define database schema. It can be Non SQL / SQL form of database instance. According to user requirement CSP will allocated the space for the user instance.

Algorithms Used

Elgamal Encryption Scheme

Key Generation phase

Input : Plain text as text data d.

Output: a,b,p,g all are private keys

Step 1: Initialize the random message from user as d. (it should be any kind of text data).

Step 2: initialize a,b,p,g for private key purpose.

Step 3: generate P as randomly base on bit length of d. so,

Ans[]=GetRandomP(d.getbyte).bitlength base on probable prime no.

Step 4: p=Ans[0]

g=Ans[1]

Step 5: Generate a using P

a=RandomA(p)

its calculate like p.bitLength()-1,Random.
Step 6: Calculate b= calculateb(g, a, p);
so, b= g.modPow(a, p);
Step 7: Key generation done

Encryption

Input : Text data d,p,b,g
Output cipher as C1,and C2.
initialize BigInteger [] rtn = {null,null};
message=d.getbytes();
[] result= ElGamal.encrypt(message, p, b, g);
[] rtn = {null,null};
k = ElGamal.getRandomk(p);
C1 = g.modPow(k, p);
C2 = m.multiply(b.modPow(k, p)).mod(p);

Decryption

Input : input c1 and c2 as cipher a and p as private keys
Output: Plain text d.
Step 1: m = C2.multiply (C1.modPow (a.negate(), p)).mod (p);
Step 2: return m.

Algorithm 1 : Hash Generation

Input : Genesis block, Previous hash, data d,

Output : Generated hash H according to given data

Step 1 : Input data as d

Step 2 : Apply SHA 256 from SHA family

Step 3 : CurrentHash= SHA256(d)

Step 4 : Retrun CurrentHash

AES

Step 1. Char[]= char.random[5]

Step 2.string Key=(string) char[]

Step 3. Return Key

Encryption

Input : Plain text p, and Private key k

Output : Cipher text C

Step 1. Generate instance of AES.

Step 2. Set encrypt mode with cipher instance.

Step 3.Convert byte[] plaintext =Plain byte [].

Step 4. [] enc= apply cipher method on (plainbyte,k)

Step 5.Encstring = apply 64 base encoder on [] enc.

Step 6.returnEncstring.

Decryption

Input : Cipher text C, key k

Output : Plain text p

Step 1. Set k as private key for decryption.

Step 2. Set decrypt mode with cipher instance.

Step 3.byte[] ks=64 base decoder on (c)

Step 4.byte [] utf=apply decipher method on (ks,k)

Step 5.plain=convert into string class (utf)

Step 6.return plain.

Process

- First data owner upload the text data like text file
- Then apply the AES 128 16 bit encryption and signature generation using secure hash function.
- Once data owner send the data to server it first receives to TTP it means Trusted Third Party, so it will generate the hash values using SHA-256 algorithm.
- Then send to service provider.
- Service provider store all the data into database.
- Client first login to system, and calculate SHA-256 keys
- If client SHA keys and TTP SHA keys are same then the client is validate for data accessing.
- Then he can generate the request to data owner for decryption keys. Once client generate the request to owner it will reflect on data owner's dashboard.
- Data owner can send the decryption keys to client.
- Data owner having control to grant and revocation for client.
- When data owner revoke the particular client then system will automatically change the existing keys.

FUTURE WORK

The part of cloud computing has brought many researchers from different fields; yet, much effort remains to reach use and the broad acceptance of cloud computing technology. The further work can be extent to study the data error

localization, which is nothing yet, at whatever point information defilement has been distinguished amid the capacity rightness confirmation, we can just about surety the concurrent limitation of information blunders, i.e., the recognizable proof of the acting mischievously server(s)..

CONCLUSION

In this project, we've proposed a cloud-based storage scheme which supports outsourcing of information that was dynamic, where the owner is really capable of upgrading and scaling and getting the information saved by the CSP, but also archiving this information on the remote servers. Also, in the event of dispute regarding data integrity, a TTP is able to decide on the party that is dishonest. The information owner applies access control for the information that is outsourced. The security characteristics of the planned system have been analyzed by us.

References

1) A. Shamir. Identity-Based Cryptosystems and Signature Schemes. In CRYPTO 1984, volume 196 of Lecture Notes in Computer Science ,pages 47–53. Springer, 1984.
2) R. L. Rivest, A. Shamir, and Y. Tauman. How to Leak a Secret. In ASIACRYPT 2001, volume 2248 of Lecture Notes in Computer Science, pages 552–565. Springer, 2001.
3) E. Bresson, J. Stern, and M. Szydlo. Threshold ring signatures and applications to ad-hoc groups. In M. Yung, editor, CRYPTO 2002, volume 2442 of Lecture Notes in Computer Science, pages 465–480. Springer, 2002.
4) J. K. Liu and D. S. Wong. On the Security Models of (Threshold) Ring Signature Schemes. In ICISC 2004, Lecture Notes in Computer Science. Springer, 2004.
5) F. Zhang and K. Kim. ID-Based Blind Signature and Ring Signature from Pairings. In ASIACRYPT 2002, volume 2501 of Lecture Notes in Computer Science, pages 533–547. Springer, 2002.
6) J. Han, Q. Xu, and G. Chen. Efficient id-based threshold ring signature scheme. In EUC (2), pages 437–442. IEEE Computer Society, 2008.
7) J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen. Forward secure identity-based signature: Security notions and construction. Inf. Sci., 181(3):648–660, 2011.
8) "Amazon.com," Amazon Web Services (AWS), 2008. [Online]. Available: http://aws.amazon.com.
9) P. P. Tsang, M. H. Au, J. K. Liu, W. Susilo, and D. S. Wong. A suite of non-pairing id-based threshold ring signature schemes with different levels of anonymity (extended abstract). In ProvSec, volume 6402 of Lecture Notes in Computer Science, pages 166–183. Springer, 2010.