International Journal of Computer Science Engineering & Technology
IJCSET
APPROVED BY
NATIONAL SCIENCE LIBRARY (NSL)
NATIONAL INSTITUTE OF SCIENCE COMMUNICATION AND INFORMATION RESOURCES (NISCAIR)
COUNCIL OF SCIENTIFIC AND INDUSTRIAL RESEARCH (CSIR)– NEW DELHI INDIA .
ISSN :2455-9091

SECRET KEY CAPACITY OF COMPOUND SOURCE MODEL AND ONE WAY PUBLIC COMMUNICATION

[1] Limi M Nair, [2] Dr A Kousalya ME.PHD
[1] PG Scholar, [2] Associate Professor,
[1] ME Computer science and engineering, [2] Computer science,
[1, 2] United Institute of technology,
[1, 2] Coimbatore.

ABSTRACT: An attribute-based access control scheme uses two-factor protection for multi-authority cloud storage systems. In our proposed scheme, any user can recover the outsourced data if and only if this user holds sufficient attribute secret keys with respect to the access policy and authorization key in regard to the outsourced data. In addition, the proposed scheme enjoys the property es of constant-size cipher text and small computation cost. Besides supporting the attribute-level revocation, our proposed scheme allows data owner to carry out the user-level revocation. The security analysis, performance comparisons, and experimental results indicate that our proposed scheme is not only secure but also practical. In proposed system we use AES algorithm to preserve privacy of data and to avoid loss in data integrity and avoid fraudulent activity we provide two kind of key. A user who holds public key can access the file content of the corresponding people. Private Key cannot be shared with others, only the data owner can hold it.

Key Words: [Attribute-based access control scheme, AES algorithm, Attribute-level revocation, User-level revocation.]

1. INTRODUCTION

CLOUD computing has been envisioned as the next generation information technology (IT) architecture for enterprises, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk . From users' perspective, including both individuals and IT enterprises, storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with location independence, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc.

While cloud computing makes these advantages more appealing than ever, it also brings new and challenging security threats toward users' outsourced data.

Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the

infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity. Examples of outages and security breaches of noteworthy cloud services appear from time to time. Second, there do exist various motivations for CSP to behave unfaithfully toward the cloud users regarding their outsourced data status. For examples, CSP might reclaim storage for monetary reasons by discarding data that have not been or are rarely accessed, or even hide data loss incidents to maintain a reputation.

2. RELATED WORKS

Communication theory of secrecy system [1]. The problems of cryptography and secrecy systems furnish an interesting application of communication theory.1 In this paper a theory of secrecy systems is developed. The approach is on a theoretical level and is intended to complement the treatment found in standard works on cryptography. There, is a detailed study is made of the many standard types of codes and ciphers, and of the ways of breaking them. We will be more concerned with the general mathematical structure and properties of secrecy systems.

Cryptography and information security [2]. The problem of generating a shared secret key S by two parties knowing dependent random variables X and Y, respectively, but not sharing a secret key initially, is considered. An enemy who knows the random variable Z, jointly distributed with X and Y according to some probability distribution P/sub XYZ/, can also receive all messages exchanged by the two parties over a public channel. It is shown that such a secret key agreement is possible for a scenario in which all three parties receive the output of a binary symmetric source over independent binary symmetric channels, even when the enemy's channel is superior to the other two channels.

Common randomness information theory and cryptography [3]. As the first part of a study of problems involving common randomness at distance locations, information-theoretic models of secret sharing (generating a common random key at two terminals, without letting an eavesdropper obtain information about this key) are considered. The concept of key-capacity is defined .Single-letter formulas of key-capacity are obtained for several models, and bounds to key-capacity are derived for other models.

We consider the generation of common randomness (CR), secret or not secret, By two user terminals with aid from a "helper" terminal.

Common randomness and secret key generation with a helper [4]. Different component of a discrete memory less multiple source. The helper aids the users by transmitting information to them over a noiseless public channel subject to a rate constraint. Furthermore, one of the users is allowed to transmit to the other user over a public channel under a similar rate constraint. We study the maximum rate of CR which can be thus generated, including under additional secrecy conditions when it must be concealed from a wire tapper. Lower bounds for the corresponding capacities are provided, and single-letter capacity formulas are obtained for several special cases of interest.

The secrecy capacity of fading channels [5] .This is the first part of a two-part paper on the information theoretic study of biometric security systems. In this paper, the design of single-use biometric security systems is analyzed from an information theoretic perspective. Fundamental trade-off between privacy, measured by the normalized equivocation rate of the biometric measurements, and security, measured by the rate of the key generated from the is identified.

The privacy-security region, which characterizes the above-noted trade-off, is derived for this case. The scenario in which an attacker of the system has side information is then considered. Inner and outer bounds on the privacy-security region are derived in this

case. Finally ,biometric security systems with perfect privacy are studied, which is shown to be possible if and only if common randomness can be generated from two biometric measurements.

3. PROPOSED MEHODOLOGY

We propose a new data access control scheme for multi-authority cloud storage systems. The proposed scheme provides two-factor protection mechanism to enhance the confidentiality of outsourced data. If a user want to recover the outsourced data, this user is required to hold sufficient attribute secret keys with respect to the access policy and authorization key with regard to the outsourced data.

In our proposed scheme, both the size of cipher text and the number of pairing operations in decryption are constant, which reduce the communication overhead and computation cost of the system. In addition, the proposed scheme provides the user level revocation for data owner in attribute-based data access control systems. Extensive security analysis, performance comparisons and experimental results indicate that the proposed scheme is suitable to data access control for multi authority cloud storage system.

3.1 METHODOLOGIES

3.1.1 Fully Homomorphic Encryption Scheme

In cryptography we generally used two different ways to do encryption either using a secret key , i.e same key is used to encrypt and decrypt , or public key where on key remains private (private key) used to decrypt and a key is public (public key) used to encrypt.

Let's describe the secret-key homomorphic scheme now.

** As we discussed above a scheme needs three algorithms KeyGen, Encrypt, Decrypt:

KeyGen : Secret Key means we only need to create one key ; In this scheme the key is an odd integer , choose from some interval [2^n-1,2^n] . Here n is what we call a security parameter.

Encrypt (p,m) : m here is a bit {0,1} , to encrypt a bit set the ciphertext as an **integer** whose **residue modulo p** has the same parity of the plaintext (m): c = p*q + 2*r + m c is odd if m = 1 c is even if m = 0 (Yes 0 is even). p is the private key we generated before, q and r are just random integers choose from a different interval than the private key one.

Decrypt (p,c): m = (c (mod p)) (mod 2) correctness: (c (mod p)) (mod 2) = (p * q + 2 * r + m (mod p)) (mod 2) = 2r + m (mod 2) = m

Example: Suppose p = 19 c = 19 * 2 + 1 (q = 2,r = 0) c = 39 | 39 mod 17 = 5 | 5 mod 2 = 1 two bit (+, *) example: Suppose p = 17, q1 = 1, r = 1, q2 = 2, r2= 2 bit 1 = 0 bit 2 = 1

c1 = p * 1 + 2 * 1 + 0 = 19

c2 = p * 2 + 2 * 2 + 0 = 39

c1 + c2 = 58 | 58 mod 17 mod 2 = 1

c1 * c2 = 741 | 741 mod 17 mod 2 = 0

3.1.2 Quick sort algorithm

Quick sort algorithm preferred sorting algorithm in application. Quick sort algorithm mainly employs the thought of divide-and-conquer method and recursive algorithm: choose a value in the sequence as the pivot, swap the appropriate value with the pivot, and then divide the sequence into two separate parts through a times of sorting operation, all values in one part are less than those in another part, then the two parts will be processed separately in the same way until the original sequence are sorted in ascending or descending order.

Suppose a sequence A[0]…A[N-1], choose a data in the sequence (often choose the data on the first or the middle position for simplicity) as a divot, then move all the data less than it before or after it and the data larger than it after or before it, thus dividing the original sequence into two parts, and all the values in one part are less than the pivot value while those in the other part are larger than the pivot value. The two parts are processed separately

in the same way; the algorithm is executed recursively until the original sequence is wholly orderly.

Quick sort algorithm can be described as follows:

Function definition: QuickSort(A[], left, right)

Step 0 if left>=right return

Step 1 set initial variable,left → i,right → j

Step 2 choose the pivot data, A[(left + right)/2] → key

Step 3 while A[j]>=key j-1 → j

Step 4 swap A[j] and key

Step 5 while A[i]<=key i+1 → i

Step 6 swap A[i] and key

Step 7 repeat step 3 and step 4, until i=j

Step 8 QuickSort(A[],left,i-1)

Step 9 QuickSort(A[],j+1,right)

4. RESULT AND DISCUSSION VARIOUS SNAPSHOTS SNAPSHOTS

Snapshot is nothing but every moment of the application while running. It gives the clear elaborated of application. It will be useful for the new user to understand for the future steps.

Figure 4.1Registration Page

Figure. 4.2Login page

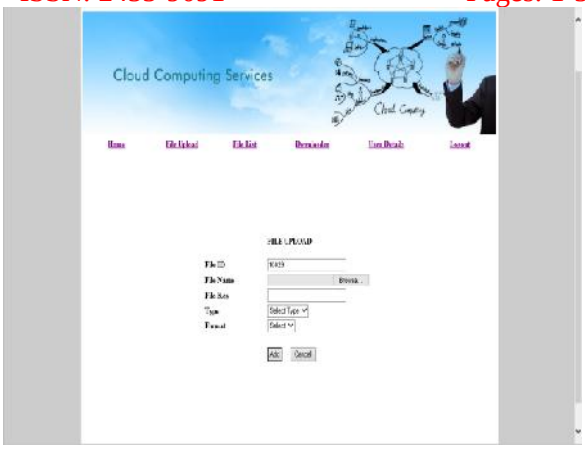

Figure. 4.3 File upload Form

Figure. 4.4 File download form

CONCLUSION AND FUTURE WORK

In this System, I investigated the problem of data security in cloud data storage, which is essentially a distributed storage system. To ensure the correctness of users' data in cloud data storage, I proposed an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete. I rely on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability.

Whenever data corruption has been detected during the storage correctness verification across the distributed servers, I can almost guarantee the simultaneous identification of

the misbehaving server(s). Through detailed security and performance analysis.

I envision several possible directions for future research on this area. The most promising one we believe is a model in which public verifiability is enforced. Besides along with our research on dynamic cloud data storage, we also plan to investigate the problem of fine-grained data error localization.

REFERENCES

[1]. Ayanthikachatterjee and Indranisengupta "Sorting of fully homomorphic encrypted cloud data":Can partitioning be effective?

[2].C.E.Shannon" communication theory of secrecy system"Bell System Technical Journal,Vol.28,pp.656-715,1949.

[3]. CsiszarandP.Naarayan"Common randomness and secret key generation with a helper,"IEEE transaction on information theory ,Vol.46,no.2,pp.344-366,March 2000.

[4]. Cwang,K.Ren,W.Lou "Towards publicity auditable secure cloud data storage services"Vol 24,no:4,2010

[5]. C.Wang,Q.Wang"Ensuring data storage security in cloud computing "Issn1548-615,August 2009

[6]. D.May,C.K.Koc "Random register remaiing to foil DPA"CHES 2001 LNCS2162 pp.28-38 May 2000.

[7].D.May,H.L.Muller "Non deterministic processor in information security "LNCS2119pp-115-129 July 2001.

[8].P.Gacs and J.K.Orner "Common information is far less than mutual information ,"Problem of control and information theory,Vol.2,pp.149-162,1973.

[9].R.Ahlswede and I.Csiszar ,"Common randomness in information theory and cryptography"-part1:Secret sharing ,"IEEE transaction on information theory" ,Vol.39,no.4,pp.1121-1132,july 1993.

[10].U.M.Maurer,"secret key agreement by public discussion from common information ,"IEEE transaction on information theory .Vol.39,no.3,pp.733-742,May 1993.