Dogo Rangsang Research Journal
ISSN : 2347-7180
UGC Care Group I Journal
Vol-9 Issue-3 Sept - Dec 2019

Compatibility Encryption with Private Key generation Approach in Cloud Computing

Mohammed Inayathulla[1], Syed Riyazul Haq[2]

[1,2]*Assistant Professor, Department of CSE*
[1,2]*Malla Reddy Engineering College (A), Hyderabad, Telangana, India.*

Abstract

Cloud computing is modern promising technology which plays a key role in feature generation of computer technology. It is broadly accepted due to few costs associated with computing while increasing scalability and flexibility for computer processes. Cloud computing users a facility of Data tasks in which different data owner is upload data and different data user is access data. Public key infrastructure (PKI) is other option to public key encryption whereas the Identity-Based Encryption IBE is public key and certificate management. The total disadvantage of IBE during revocation is the overhead computation at private key generator (PKG). In this paper handling the basic model of Identity renouncement. We generate pseudonym for each user to hide users permit identity. This project development which is provable secure under the as of late formulized Refereed Delegation of Computation system. The proposed data storage security system user's data security by using encryption, user authentication; re-encryption and this model provide security against DDOS attack. Data owner useful this proposed model provides security for online notification of user give request in the form of SMS to online all the time.

Index Terms: *Cloud Computing, DDOS, Identity Based Encryption, Outsourced data, Security, Attribute Based Encryption, Pseudonym.*

1. Introduction

Identity based encryption model takes any user to generate a public key from a known identity value such security string [1]. There is trusted third party called the Private Key Generator (PKG) the uses corresponding private keys. For encryption and decryption operations, PKG first publishes security public key, and generate the corresponding users private key Using this master public key, any user can generate a public key corresponding to the identity by combining the master public key with the identity value. To get a corresponding private key, authorized user can use identity ID contacts PKG, which uses the master private key to generate private key for identity ID. As a result, user can encrypt messages with no prior distribution of keys between participants [2]. This is very useful in cases where redistributions of keys is inconvenient because of technical restraints. However, for decryption of message, the authorized user must obtain an appropriate private key from PKG. In this approach the problem is that PKG must be highly trusted, as it has ability to generate any users' private key and decryption of message without authorization. Because any user's private key can be generated using third party's secret, this system has inherent key assurance [3]. Although still at its early stage, Cloud Computing has already drawn great attention, and its benefits have attracted an increasing number of users to outsource their local data centers to remote cloud servers. Data security is a critical issue for remote data storage. In particular, this system using a novel cryptography Identity Based Encryption (IBE) and encryption and enhance it toward providing a full fledged cryptographic basis for a secure data sharing scheme on un trusted storage [7]. To prevent unwanted disclosure of sensitive information, data

owners may have to encrypt their data before outsourcing. In this, only the authorized users with the decryption keys can recover the data, and other unsolicited accessory cannot decrypt the data without the decryption keys the cloud service provider (CSP), cannot execute decryption [8] even if they successfully obtain the cipher-texts stored in the cloud [3]. Including, this system also present one of the solutions for securing data server against DDOS attack which may more commonly happens in Cloud Computing [9].

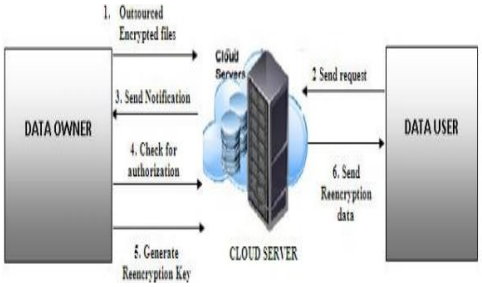

Fig. 1. Security Enhancement of Cloud Data Storage

2. Related Work

An Identity-Based Encryption (IBE) is an interesting alternative to public key encryption, which simplify key management in a certificate-based Public Key Infrastructure (PKI) with use of human-intelligible identities (e.g., unique name, IP address ,email address, etc) as a public key. D. Boneh and M. Franklin propose a fully functional identity-based encryption scheme (IBE). The scheme has chosen cipher text security in the random oracle model assuming an elliptic curve variant of the computational Diffie-Hellman problem. System is based on the Weil pairing and give precise definitions for secure identity-based encryption schemes and give several applications for such systems [1].

A. Sahai and B. Waters introduce a new type of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE an identity Is viewed as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ID, to decrypt a cipher text encrypted with an identity, ID' , if and only if the identities ID and ID',are close to each other as measured by the set overlap distance metric [2]. The availability of fast and reliable Digital Identities is an essential ingredient for the successful implementation of the public-key infrastructure of the Internet. All digital identity schemes must include a method for revoking someone's digital identity in the case that this identity is stolen before its expiration date (similar to the cancelation of credit-cards in the case that they are stolen).

W. Aiello, S. Lodha, and R. Ostrovsky proposed an elegant method of identity revocation which requires very little communication between users and verifiers in the system They reduced the overall CA to Directory communication, while still maintaining the same tiny user to vendor communication [3] we arrange OIRS under the compacted identifying framework, which is known for its ease of restricting together the routine inspecting and weight for picture securing. Data proprietors simply need to outsource stuffed picture tests to cloud for diminished stockpiling overhead. Besides, OIRS, data customers can handle the cloud to securely imitate pictures without revealing information from either the compacted picture tests or the crucial picture content. This process starts with the OIRS arrangement for insufficient data, which is the customary application circumstance for pressed identifying, and after that show its normal development to the general data for essential exchange offs amidst productivity and precision. This separates the security confirmation of OIRS and conduct wide examinations to display the structure

feasibility and effectiveness. For satisfaction, it moreover inspects the ordinary execution speedup of OIRS through gear collected in structure layout [11] the structure practicality and productivity. For satisfaction, this looks at the ordinary execution speedup of OIRS through hardware collected in structure plot.

3. Proposed Work

With the fast improvement of adaptable cloud administrations, it turns out to be progressively defenseless to utilize cloud administrations to share information in a companion circle in the distributed computing environment [12]. Since it is not attainable to execute full lifecycle protection security, access control turns into a testing assignment, particularly when we share information on cloud servers. Keeping in mind the end goal to handle this issue, we propose time determined qualities, a novel secure information self-destructing plan in distributed computing. Though, prior the information would not get erased consequently from cloud. In proposed framework the information gets erased from the cloud and space is made [13].

In this proposed system User registration is done as well as login with valid credentials. After login user get the keys from key service provider based on identity. The user encrypts the file using the architectural view represents same key and upload it at cloud server. When the user gets removed from the organization then the revocation takes place and key gets updated to provide security. The self-destructive scheme is implemented to delete the data or files automatically after completion of time span [14]. we design a method in which each user takes a different pseudonym when accessing cloud services.

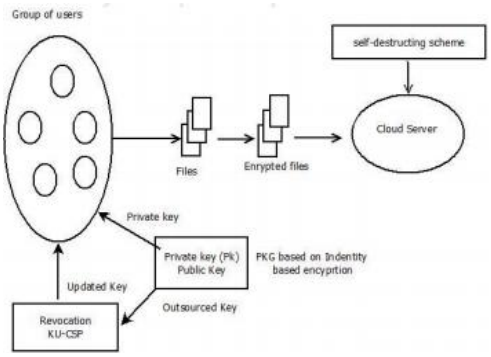

Fig. 2. Architectural view of proposed system.

There is almost no relationship between a user identity and a corresponding pseudonym is provided, and no relationship is provided between the pseudonyms for a single. Pseudonym use will not affect user's attestation also reduces the amount of input data representing private user information thus making it almost impossible for attackers to attack on users. In cloud data is stored remotely, user is not aware of any security threat [6]. Data modification can do by the untrusted server ,unauthorized user or by some malicious activity. So, user needs to be ensured that their data are intact. For this it is important to check integrity of data. for this proposed system generate meta data and using this meta data we examine the accuracy of data

3.1. Proposed Algorithms

There are several reasons like Reduction of costs, Universal access and many more because of which cloud computing is so widely used among businesses today. Thus, it require a new working paradigm for introducing cloud services into IBE revocation to fix the issue of efficiency and storage overhead. A naive approach is hand over the private key generators (PKG) master key to the Cloud Service Providers (CSPs). [4]The CSPs then simply update all private keys by using the traditional key update technique and transfer the private keys to unrevoked users. However, this approach is based on an unrealistic assumption that CSPs are fully trusted and are allowed to access the master

key for IBE system. But, in practice the public clouds are likely outside of the same trusted domain of users and are curious about users individual privacy. For this reason, [6] a challenge is how to design a secure revocable IBE scheme so that we can reduce the overhead computation at PKG with an untrusted CSP is raised.

A. Pseudonym Generation algorithm

1. User Identity ID is given as initial input.

2. Check whether pseudonym is already generated or not.

3. If yes then give message pseudonym is already generated.

4. If not chose type of pseudonym Alpha/Numeric/Alphanumeric.

5. Use random function to generate random number.

6. Generate pseudonym using random number generated in step 5.

7. Return pseudonym.

The system is Pseudonym Generation Scheme with Combining the Identity based encryption and Attribute-based Encryption with Outsourced Revocation in Cloud Computing. We use multiple KU-CSP for key updating. For data security use an efficient encryption algorithm. For integrity checking, generate meta data before upload the data in cloud. Using the Meta data the integrity of the file is verified. We design a method in which each user takes a different pseudonym when accessing cloud services. There is almost no relationship between a user identity and a corresponding pseudonym is provided, and no relationship is provided between the pseudonyms for a single. Pseudonym use will not affect users attestation also reduces the amount of input data representing private user information thus making it almost impossible for attackers to attack on users. In cloud data is stored remotely, user is not aware of any security threat. Data modification can done by the un trusted server unauthorized user or by some malicious activity. So user needs to be ensured that their data are intact. For this it is important to check integrity of data. for this proposed system generate meta data and using this meta data we examine the accuracy of data.

B. Key Generation Algorithm

1. Select randomly two large prime number p,q

2. Compute n=p*q. Where n is modulus used to generate public key and private key.

3. Compute the function as $\Psi(n) = (p*1)(q*1)$.

4.Select any random number e between 1 and (n) the function value previously calculated in step 3 such that the number is co-prime to '(n) and is not divisor of Ψ (n).

5. Calculate d, which represent modular multiplicative inverse of e mod Ψ (n). i.e. d should satisfy equation e*d mod Ψ (n) =1.

6. Private key is represented by d calculated in step 5

The proposed an elegant method of identity revocation which requires very little communication between users and verifiers in the system They reduced the overall CA to Directory communication, while still maintaining the same tiny user to vendor communication [5].

C. Hierarchical Attribute-Base Encryption (HABE)

This scheme (HABE) proposed by Wang et al [10]. It is a combination of Hierarchical Identity Base Encryption (HIBE) and CP-ABE. It provides fine grained access control, full delegation and high performance. The HABE scheme consists of many attribute authorities and many users. ABE uses disjunctive normal form policy. The same attribute

may be administrated by multiple domain masters according to specific policies, which is most complicated to implement in practice. HABE [10] model consists of a Root Master (RM) and multiple domains. One domain consists of number of domain masters and number of users related to end users. HABE model It is mainly applicable to the environment of enterprises sharing data in cloud. This scheme has issues with multiple values assignments and practical implementation is very difficult because same attribute may be administered by different domain masters

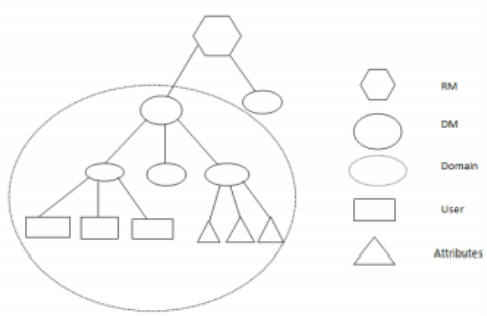

Fig. 3. HABE model

D. Attribute-Based Broadcast Encryption (ABBE)

Broadcast systems means distribute file systems or commercial content to a large set of users. In Broadcast Encryption scheme [14] allows the broadcaster to select or revoke not only the single users, but groups of users defined by their attributes. In this scheme access policy are restricted and efficient decryption is allowed. The restriction of access policy is enough to provide broadcast encryption since the OR function can be simulated using concatenation, exactly like in the Subset-Cover framework. This scheme has the ability to compute a specific greatest common divisor of polynomials. Each user is associated with a polynomial and a cipher-text is associated with another polynomial. A user in the access policy is defined by a cipher text computes the greatest common divisor of its polynomial and of the polynomial associated with the cipher text: this divisor is the same for all users in the access policy. A receiver not in this access policy would obtain a different polynomial: this polynomial cannot be computed, or it cannot be used to decrypt the cipher text. . In their scheme, the authors however use an individual receiver-specific attribute and the disjunction is obtained by concatenation of several instances of the encryption scheme. Advantage of the Attribute Based Broadcast Encryption is it handles the both Cipher text-policy and key policy in efficient manner [11]. ABBE scheme is the strong collision resistant at the handling of cipher text [13]. It overcomes the limitations on ABE. The major advantage of the ABBE scheme is it's also possible to integrate the Identity i.e. Identity Based Broadcast encryption technique is better way to provide the authentication as well as confidentiality [2]. For the PHR System Attribute Based Broadcast Encryption technique is the better technique to protect the Records.

4. Experimental Results

In this section we provide the Results on basis of Construction of Proposed system. We evaluate Time required to respond by single CSP compared to time required by multiple CSP. The existing System uses single system to generate keys named CSP central. So According to performance evaluation for about 20 Users time taken by single CSP is approx. 1000(ms).In Proposed system we make use of multiple CSP. Expected time taken by 2 or more CSP for about 20 users is expected to reduce to 500 ms

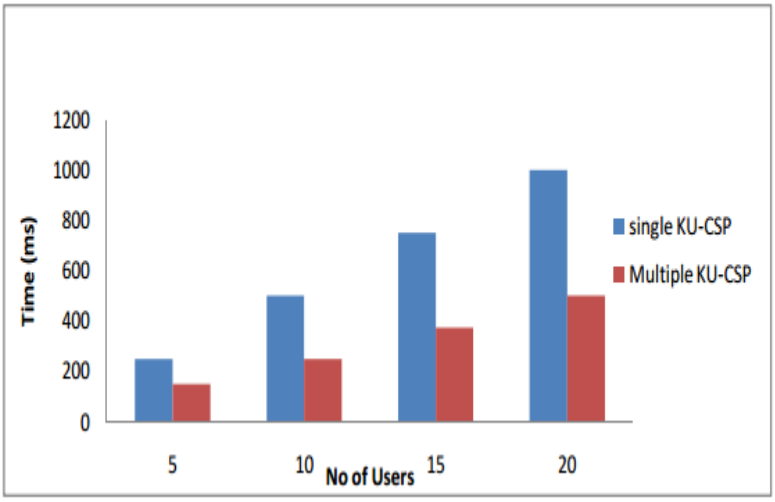

Fig. 4. Comparison between Single and Multiple KU-CSP

5. Conclusions

Cloud computing is a distributed system where different users of different domains can share data among each other. Different Identity-based proxy re-encryption schemes have been proposed to outsource sensitive data from the owner to an external party. Nevertheless, they cannot be employed in cloud computing. Security of data storage is more important in cloud. The proposed system enhances the security of data storage by introducing the identity based secure encryption and re-encryption. It provides many advantages like online notification in the form of SMS on owners' registered mobile number. So no need to be online all the time this system overcome the previous schemes and also provides security against Distributed Denial of Service attack and it provides secure model of cloud storage with safe data uploading. Focusing on issue of identity revocation, we have introduced outsourcing computation into IBE and proposed a revocable scheme in which the revocation operations are delegated to CSP. User needs not to contact with PKG during key-update, in other words, PKG is allowed to be offline after sending the revocation list to KU-CSP. It does not require secure channel or user authentication during key-update between user and KU-CSP. We combine the Identity based and Attribute-based Encryption which will provide more security to user. For integrity checking, generate meta data before upload the data in cloud. Using this meta data the integrity of the file is verified.

References

[1] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology (CRYPTO'98). New York, NY, USA: Springer, 1998, pp. 137–152

[2]. D. Boneh and M. Franklin, Identity-based encryption from the weil pairing, in Advances in Cryptology CRYPTO 2001, Springer Berlin / Heidelberg, 2001, vol. 2139, pp. 213 229.

[3]. A. Sahai and B. Waters, Fuzzy identity-based encryption, in Advances in Cryptology EUROCRYPT 2005 , Springer Berlin / Heidelberg, 2005, vol. 3494, pp. 557557.

[4]. W. Aiello, S. Lodha, and R. Ostrovsky, Fast digital identity revo-cation, in Advances in Cryptology CRYPTO98.Springer, 1998.

[5]. V. Goyal, Certificate revocation using fine grained certificate space partitioning, in Financial Cryptography and Data Security , Springer Berlin / Heidelberg, 2007, vol.4886, pp. 247259.

[6]. F. Elwailly, C. Gentry, and Z. Ramzan, Quasimodo: Efficient certificate validation and revocation, in Public Key Cryptography PKC 2004 , ser. Lecture Notes in Computer Science, F. Bao, R. Deng, and J. Zhou, Eds. Springer Berlin/ Heidelberg, 2004, vol. 2947, pp. 375388.

[7] Pierangela Samarati and Sabrina De Capitani di Vimercati, ”Data Protection in Outsourcing Scenarios:Issues and directions”, E-Business and Telecommunications: 6th International Joint Conference, ICETE ,2011.

[8] Carl Youngblood, ”An Introduction to Identity-based Cryptography”, CSEP 590TU,University of Washington Online Course, free tutorials and lecture notes, March 2005

[9] Song Luo, Jianbin Hu and Zhong Chen, ”New Construction of Identity-based Proxy Re-encryption”, International Association for Cryptologic Research ,2010

[10] Lanjuan Yang,Tao Zhang ; Jinyu Song ; Jin Shuang Wang, ”Defense of DDoS attack for cloud computing” ,IEEE International Conference on Computer Science and Automation Engineering (CSAE),(Volume:2) ,2012

[11]. [10]Dan Boneh, Matthew Franklin, “Identity-Based Encryption from the Weil Pairing”, Appears in SIAM J. of Computing, Springer-Verlag, 2001.

[12]C. Gentry, “Practical identity-based encryption without random oracles,” in Advances in Cryptology (EUROCRYPT‟06), S. Vaudenay, Ed. Berlin, Germany: Springer, 2006, vol. 4004, pp. 445–464.

[13]C. Gentry, C. Peikert, and V. Vaikuntanathan, “Trapdoors for hard lattices and new cryptographic constructions,” in Proc. 40th Annu. ACM Symp. Theory Comput. (STOC‟08), 2008, pp. 197–206.

[14]S. Agrawal, D. Boneh, and X. Boyen, “Efficient lattice (h)ibe in the standard model,” in Advances in Cryptology (EUROCRYPT‟10), H. Gilbert, Ed. Berlin, Germany: Springer, 2010, vol. 6110, pp. 553–572.

