International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Pseudonym Generation with Combining the Identity Based and Attribute Based Encryption with Outsourced Revocation in Cloud Computing

Kirti Patil[1], Sonali Patil[2]

[1]M.E. student, Dept. of Computer Engg, BSIOTR, Savitribai Phule Pune University, India
[2]Assistant Professor, Dept. of Computer Engg, BSIOTR, Savitribai Phule Pune University, India

Abstract: ***Identity Based Encryption (IBE) simplifies public key management and certificate management at Public Key Infrastructure (PKI) with help of Private Key Generator (PKG). However, one of the main drawback of IBE is overheaded computation at PKG during user revocation. The use of Key update cloud service provider (KU-CSP) offloads most of key generation operations during key-issuing and key-update process leaving only a number of simple operations for PKG and users to perform locally. For this, we generate a hybrid private key for each user, in which an AND gate is used to connect and bound the identity component and time component. But KU-CSP is untrusted. So, we propose a Pseudonym Generation Scheme for Identity based Encryption and Outsourced Revocation in Cloud Computing. We generate pseudonym for each users to hide user's original identity. Along with this we increase the security by combining the techniques Identity Based Encryption and Attribute Based Encryption. Also we use multiple KU-CSP for load balancing purpose. For integrity checking, we generate signature before uploading the data in cloud. Using this signature integrity of the file is verified.***

Keywords: Identity Based Encryption, Attribute Based Encryption, Pseudonym.

1. Introduction

Identity based encryption system allow any user to generate a public key from a known identity value such as an ASCII string. There is trusted third party, called the Private Key Generator (PKG), who generates the corresponding private keys. For encryption and decryption operations, PKG first publishes a master public key, and then generate the corresponding master private key (referred as master 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. This is very useful in cases where predistribution 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 user's 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.

Different systems have been proposed which remove this including certificate-based encryption and secure key issuing cryptography. In PKI setting, revocation is done by appending validity periods to certificates or using combinations of techniques. But, this require management of certificates which is precisely the burden that IBE strives to alleviate. Boneh and Franklin suggested that their private keys can renewed by user periodically and senders use receivers identity with current time period. But this mechanism would results in an overhead at PKG. In another word, all the users even though their keys have been revoked or not, have to contact with private key generator(PKG) periodically to prove their identities and update new private keys. It is needed that PKG must be online and the secure channel has to be maintained for all the transactions, which will become a bottleneck for IBE system as the number of users grows. Many businesses large and small use cloud computing today either directly or indirectly instead of traditional onsite alternatives.

There are a number of reasons like Reduction of costs, Universal access and many more because of which cloud computing is so widely used among businesses today. Thus it requires 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). 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 user's individual privacy. For this reason, 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.

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 keys.

Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia and Wenjing Lou have proposed Identity-based Encryption with Outsourced Revocation in Cloud Computing. They proposed Key update cloud service provider for updation of key so that user need not to contact every time to private key generator for private key.

D. Boneh and M. Franklin propose a fully functional identity-based encryption scheme (IBE). The scheme has chosen ciphertext 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 [2].

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[3].

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[4].

3. Implementation Details

3.1 Problem Statement

How to reduce the overhead computation at PKG with an untrusted KU-CSP in cloud computing environment and to ensure that the stored data is not compromised.

3.2 Existing System

Identity-Based Encryption (IBE) is an effective option available to public key encryption, which is proposed to simplify the key management in a certificate-based Public Key Infrastructure (PKI) by using Users identity (e.g., unique name, email address, IP address, etc) as Public key Pk.

The existing system uses IBE i.e identity of user as public key and key update cloud service provider (KU-CSP) for updation of private keys so that user only once need to contact Private Key Generator (PKG).This will reduce overload on PKG.

The disadvantage of the existing system is as KU-CSP has keys he can use or share users confidential data without users permission. So we cannot fully trust on KU-CSP ie KU-CSP is untrusted. Also as number of users grows requests of users are going to increase. So single KU-CSP may become overloaded so responding time will be increased. Also user must be able to check integrity of his/her data to know any alteration or modification is done on data.

3.3 Proposed System

The proposed system is Pseudonym Generation Scheme with Combining the Identity based encryption and Attribute-based Encryption with Outsourced Revocation in Cloud Computing.

In proposed work, we design a method in which each user takes a different pseudonym when accessing cloud services. We are using Psedonym to hide user identity so that KU-CSP cannot identify user. 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.

we use multiple KU-CSP for key updation So that load is divided and KU-CSP will not be overloaded. For integrity checking, generate meta data before upload the data in cloud. Using the meta data the integrity of the file is verified.

4. Architecture and Module

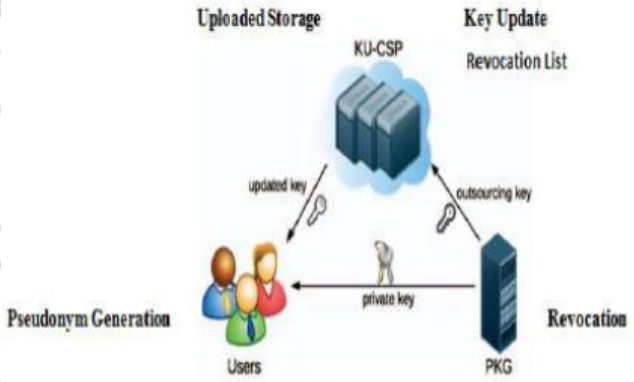

Figure 1: Architecture of Proposed System

The above Figure 1 represents the architecture of proposed system. The flow and description of each the modules present in the system discussed as below.

1. Pseudonym Generation: we generate pseudonym for each user. It takes users identity and provide pseudonym. Pseudonyms are usually taken or adopted to hide an individual ones real identity, for example writers' pen names, or terrorists, and computer hackers fake names. Here we use pseudonym for hide users real identity. Because KU-CSP is untrusted. So adversaries can use the data without permission based on user's identity.

2. Key Generation: For each user's private key request on identity ID, PKG firstly checks whether the request identity ID exists in revocation list RL, if so the key generation is aborted. Then it generates Private Key (PK) and Outsourcig Key (OK).finally, it sends Private Key to user and Pseudonym with Outsourcing key to KU-CSP respectively.

3. Encryption: user wants to upload any file or message to KUCSP. But KU-CSP is untrusted. So encryption is compulsory. For security we use attribute based encryption with identity based encryption scheme. Here a user can encrypt a message M under Pseudonym P with attributes and time period Ti. This provides the ciphertext (CT). Then user

can upload this ciphertext to KU-CSP.

4. Decryption: user wants to download any file or message from KU-CSP. Users uses his private key send by PKG and decrypt the message. Here the ciphertext CT is encrypted under P with attributes and Ti, and the user has a private key PK, this provides original message M.

5. Key Updation: Upon receiving a key-update request on pseudonym, firstly KU-CSP checks whether ID exists in the revocation list RL, if so KU-CSP returns null and key-update is aborted. Otherwise it returns Updated Key to user.

5. Algorithms Used

1) 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 Use random function to generate random number.
5. Generate pseudonym using random number generated in step 4.
6. Return pseudonym.

2) AES (Advanced Encryption Standard) Algorithm

Steps of AES Encryption Process

Step 1: Byte Substitution (SubBytes)
Step 2: Shiftrows
Step 3: MixColumn
Step 4: Addroundkey

Steps of AES Decryption Process

The process of decryption of an AES cipher text is similar to the encryption process step in the reverse order. Each round consists of the four processes conducted in the reverse order.

6. Result

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.

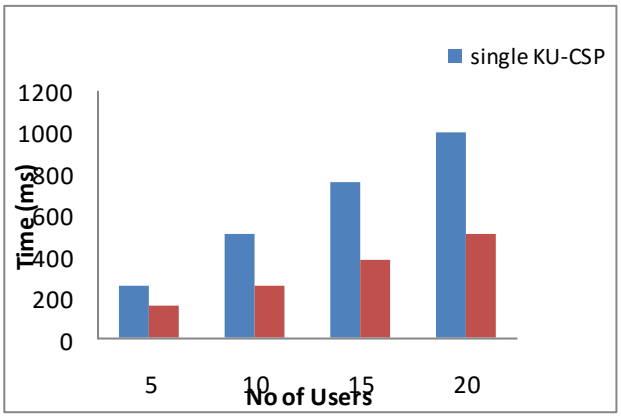

Figure 1: Comparison between Single and Multiple KU-CSP

The existing System uses single system to generate keys named CSP i.e. 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 i.e. (2or3).Expected time taken by 2 or more CSP for about 20 users is expected to reduce to 500 ms.

7. Conclusion

Focusing on issue of identity based encryption, we have introduced pseudonym so that we will provide security to user by hiding identity of user from KU-CSP. User needs not to contact with PKG for key-update, in other words, PKG is allowed to be offline after sending the revocation list to KU-CSP. It do 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 signature of data. Using this signature data the integrity of the file is verified.

References

[1] Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia and Wenjing Lou, 'Identity-based Encryption with Outsourced Revocation in Cloud Computing', IEEE 2015.
[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.

Author Profile

Ms. Kirti Patil Received degree of BE from Shivaji University, Kolhapur in 2011 and pursuing ME Computer Engineering from JSPM's BSIOTR, Savitribai Phule Pune University.

Prof Mrs. Sonali Patil M.Tech CSE, PhD pursuing from BSAU, Chennai. Asst. Prof Department of Computer Engineering JSPM'S BSIOTR, WAGHOLI, PUNE