International Journal of Latest Trends in Engineering and Technology Special Issue SACAIM 2016, pp. 577-582
e-ISSN:2278-621X

CONSTRAINED CLOUD SECURITY: CONTACT CONTROL APPROACH

S.Gowtham[1], P.Saravanan[2] and S.Vignesh[3]

Abstract - Today's world is all about easy and quick accessing the entire thing we need. Especially when it comes to computing and accessing data resources it must be rapid. In order to access the data anywhere at any time the cloud computing is the bliss in this fast world to either share or outsource whatever we have. Storing is not necessarily done in the personal or owners device. All the data are stored, maintained and served whenever the user wants it through a cloud server. The users are opting to store all their data into a third party server either it may be critical or not. So these cloud servers must be protected in the way none can able to touch those both critical and non critical data. In order to increase the protection contact control approach is what proposed to prevent unapproved access and making more secured even the approved ones. Every proxy is re encrypted based on its identification and after it can be stored into the cloud by substitution cipher.

Keywords – Cloud, Entry control, Proxy Re- Encryption, substitution cipher.

I. INTRODUCTION

Cloud can be defined as a network or Internet which provides global sharing of data all over the world independent of time, place and any other requirements. In other words it can be defined as a remote server maintained by a third party. Cloud services can be used in public networks, private networks such as WAN, LAN or VPN. All web applications such as e-mail, web conferencing, customer relationship management (CRM), business management, data outsourcing and everything can be done in cloud. Cloud Computing [1] refers to manipulating, configuring, and accessing of applications online. It offers many services such as online data storage, infrastructure and application based on the user's requirement. Hence it is also called as on –demand service model.

II.SECURITY ISSUES

Even though cloud computing has opened new approach in the networking world, It also have some pitfalls with concern to security. Some of the issues are discussed below:
While considering the data security the focus is made on Confidentiality, Integrity, Availability, Authenticity, Authorization, Authentication and Non-Repudiation [18].

[1] *Department of Information Technology Dr.N.G.P.Institute of Technology, Coimbatore, Tamilnadu, India*
[2] *Department of Information Technology Dr.N.G.P.Institute of Technology, Coimbatore, Tamilnadu, India*
[3] *Vakilsearch.com, Chennai, tamilnadu, India*

- *Data Confidentiality:* This is an important property of data which ensures the enclosure of data to the authorized user.
- *Data Integrity:* This property ensures that the data stored in the remote server is not modified.
- *Data Availability:* This property ensures that the data is available to the legible users whenever they need it.
- *Authorization & Authentication:* Both of these properties are look alike. Whenever a registered user request access to a resource he is said to be authenticated user. And whenever a user sent message he has to ensure his identity by using digital signature and etc. This process is called authorization [19].
- *Non-Repudiation:* Non-Repudiation is the process that ensures s that the data is sent and received between the authorized users while communicating.
- *Location of the data:* There must be assurance that the data, including all of its copies and backups, is stored only in geographic locations permitted by contract, SLA, and/or regulation. For instance, use of "compliant storage" as mandated by the European Union for storing electronic health records can be an added challenge to the data owner and cloud service provider
- *Data backup and recovery schemes for recovery and restoration***:** Data must be available and data backup and recovery schemes for the cloud must be in place and effective in order to prevent data loss, unwanted data overwrite, and destruction. Don't assume cloud-based data is backed up and recoverable.
- *Data discovery:* As the legal system continues to focus on electronic discovery: cloud service providers and data owners will need to focus on discovering data and assuring legal and regulatory authorities that all data requested has been retrieved. In a cloud environment that question is extremely difficult to answer and will require administrative, technical and legal controls when required [10].
- *Data aggregation and inference:* With data in the cloud, there are added concerns of data aggregation and inference that could result in breaching the confidentiality of sensitive and confidential information. Hence practices must be in play to assure the data owner and data stakeholders that the data is still protected from subtle "breach" when data is commingled and/or aggregated, thus revealing protected information.

III. PROPOSED SYSTEM OVERVIEW

Due to the dynamic network topology of networks the existing security proposals presented which could achieve both of the confidentiality and data access control may not be suitable in dynamic cloud computing . Specifically, the attribute based encryption or multi-recipient encryption which is more suitable for a static and small-scale network rather than for the dynamic network and potentially comprised of millions of users who could join or leave the network arbitrarily. Moreover one user may possess many attribute and conversely one attributes may be possessed by many users which makes the data owner difficult to set up the correspondence between the users and attributes. These observations motivate us to propose a novel data service mechanism in dynamic cloud computing.

IV. SECURITY MODEL

In this proposed system, a user-efficient and secure data service mechanism in dynamic cloud computing, which enables the users to enjoy a secure outsourced data services at a minimized

security management overhead. The core idea of project is that it outsources not only the data but also the security management to the mobile cloud in a trusted way. To achieve this, we adopt an identity-based proxy re-encryption scheme which allows a mobile user to encrypt his data under his identity to protect his data from leaking and, at the same time, to delegate his data management capability to the mobile cloud. Furthermore the mobile user could delegate his access control capability to the cloud, which could grant the access of an authorized user by transforming the cipher text encrypted with the data owner's identity to the one with the sharer's identity[4].

For that proxy re-encryption the cloud uses the secret key of the sharer who is an authorized user had already registered with the data owner. So that it could be decrypted by sharers in the future using their secret key generated based on their identity. And different sharer's identity corresponding to different proxy re-encryption key is generated at the time of their registration. Given the proxy re-encryption key by the owner, the cloud can convert the cipher text outsourced by the data owner to the cipher text that can be decrypted by the sharer.

As mentioned above, in this proposal the role of the cloud is:

- Providing secure storage for the users.
- Serving as the secure proxy.

From the perspective of the user, the task of convert cipher text is relinquished to the cloud, and the user just only needs to upload a key whose size is far less than the whole file[1].

Our Protocol

The illustration is given in Figure 3.1. In this the data owner uploads the encrypted file to the cloud. Then the cloud performs the Proxy - Re encryption using the sharer's identity and stores it in the database. Whenever the user wants to access the file he retrieves it by decrypting the file using his secret identity.

Module Description

The major modules of this project are as illustrated as following:

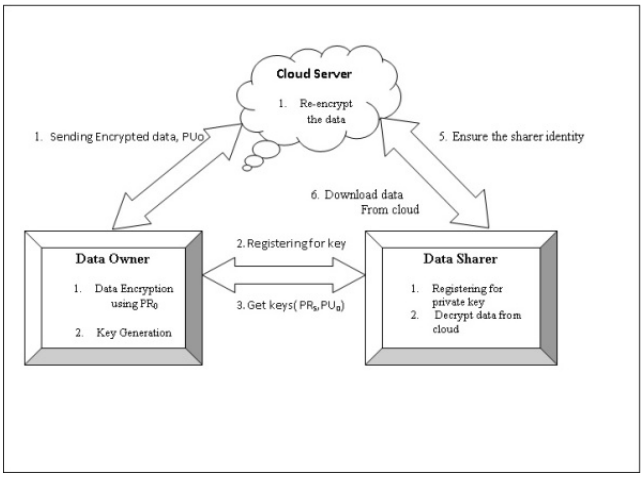
- System Set up
- Data Encryption
- Data sharing
- Proxy re-encryption.
- Data Access

System set up

In this phase, two important tasks are done.

- The system setup
- Key Generation.

In the system set up, the system parameters are built up. The system is to guarantee the authorized sharers who can access the data. In the Key Generation phase a pair of keys is generated for the data owner using a public key cryptographic algorithm. Here I adopted a public cryptography algorithm at the owner side. A pair of keys **(PUo**, **PR_o)** is generated. In this each user needs to register with the system using his identity to obtain a secret key corresponding to his identity. The data owner can share his public key (PU_o) only with the identity of the registered shares[5].



1.1 System model

Data Encryption

In the data encryption phase the data owner runs the Encrypt algorithm which convert the plain text M(F) into cipher text C(F) using his private key(Pro). As mentioned in the previous phase the keys for encryption are generated whenever the data owner choose a file for uploading. The data owner performs a first level encryption using a public key cryptographic algorithm with his private key (PRo) after that the cipher text can be transformed to the cloud where a second level encryption (IB-PRE) is performed.

C (F) =Encrypt (M (F), Pro)) (1)

Whenever the data owner encrypted the data, it will be uploaded in the cloud.

Identity Based Proxy Re-Encryption

This process is done in the cloud to provide a second level of security. In this process the cloud server uses the data owner's public key to perform the Proxy Re-Encryption and ensures the two level of security. The cloud does not have any knowledge about the data shared by the data owner. Other than the Public key (PUo) of data owner the cloud don't know anything about the data which in turn restrict the access of original data even by the cloud server.

R (F) = Encrypt(C (F),PUo) (2) (3.2)

Data Sharing

In this phase any user who want to gain access of data shared by the data owner have to register with the data owner and get a pair of keys such as a secret key(PRs) which is based on the sharer's identity and the public key of the data owner(PUo).

The secret key or the sharer's private key is generated using the hash function.

PRs= H (IDu) (3)

This key pair is used by the sharer for accessing the data stored in the cloud server.

Data Access

Whenever the sharers want to access the data in the cloud server [6], he needs to ensure his identity in the cloud server. After the verification process the cloud server let the sharer to download the data which is dually encrypted. The sharer decrypt the second level of encryption which is made by the cloud using the data owner's public key (PUo).

R(F)→ Decrypt(R(F),PUo)→C(F) (4)

After that the sharer has to use his private key to decrypt the first level of encryption made by the data owner.

C(F)→Decrypt(C(F),PRs) (5)

Thus the system is adapted to provide high security by implementing the security in two levels.

Advantages of the proposed system

- As the data owner only has control of key generation there will be no abuse of data in the cloud server.
- Since this algorithm provides two levels of security there will be improved than the existing algorithms.
- As the secret key is only shared with the authorized users there will be no un authorized access compared to the existing algorithm.

This algorithm is more flexible that any number of users can be accommodated and update of access keys can be made easily.

V.EXPERIMENT RESULTS

As the scheme relatively reduces the communication overhead this in turn reduces the computation cost. The reduction of communication overhead is shown in the following graph by making ratio between the transferred file size and the number of users.

In the Multi Recipient algorithm the data transferred to cloud is the data which is encrypted n times for n number of users individually and then the whole data is transmitted[7].

The data transferred to cloud can be calculated as

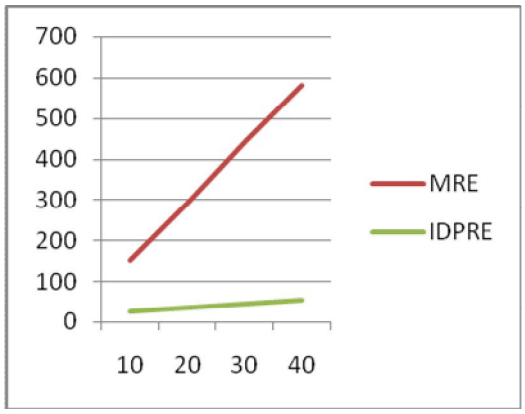
$$\text{Transferred data} = \sum_{i=0}^{n} ([E(Ki,M)]) \quad \text{for } i=1 \text{ to } n$$

In this M is the data file which is to be encrypted. Ki is the secret key of the user i. E(Ki,M) is the data file encrypted using the ith user's secret key.

In IB-PRE the transferred data consists of the encrypted [6] file and the key of the user at his time of registeration. Here the transferred data can be calculated as

$$\text{Transferred data} = E(PRa,M) + \sum_{i=0}^{n} PRsi$$

In this E (PRa,M) is the encrypted data file with the owners private key. PRa is the private key of the data owner, PRsi is the secret key of the i-th user.



1.2 Comparison of MRE and IB-PRE

VI.CONCLUSION

This project explored an identity based proxy re-encryption scheme to make the users easily implement fine-grained access control of data and also guarantee the data privacy in the cloud. At the same time, the cost of updating of access policy and communication is also reduced in this mechanism.

As the keys are generated only by the administrator there will be no abuse of keys. Each user has an identical key based on their identity there will be no duplicates. Each user is registered with the Administrator and the secret key is only known to the user and owner there will be no unauthorized access. As the data is forwarded to the cloud in encrypted format, it does not have any knowledge about the data. Though the hackers get the data from the cloud they don't know the logic and cannot decrypt the data [2]. As the encrypted data and keys only transferred the computation cost will be comparatively low. There will no limitation in the number of the sharer.

VII.FUTURE WORK

This work can be extended to improve the performance by reducing the time taken to calculate the keys for data owner and the data sharer individually adopting some alternate techniques.

REFERENCES

[1] Weiwei Jia *yz*, Haojin Zhu*y*, Zhenfu Cao*yx*, Lifei Wei*y*, Xiaodong Lin "A Secure Data Service Mechanism in Mobile Cloud Computing"

[2] S.Yu, C.Wang, K. Ren, and W.Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in INFOCOM 2010, pp. 534

[3] S. Creese, P. Hopkins, S. Pearson, and Y. Shen, "Data protection-aware design for cloud services," in CloudCom, 2009, pp. 119–130.

[4] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-based access control models," Computer, vol. 29, no. 2, pp. 38–47, 2002.

[5] R. Sandhu and P. Samarati, "Access control: principle and practice," Communications Magazine, IEEE, vol. 32, no. 9, pp. 40–48, 2002.

[6] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in VLDB, 2007, pp. 123–134.

[7] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615,nb2003.

[8] R. Curtmola, O. Khan, R. C. Burns, and G. Ateniese, "Mr-pdp: Multiple replica provable data possession," in ICDCS, 2008, pp. 411–420.

[9] Ruoyu Wu, Xinwen Zhang, Gail-Joon Ahn, Hadi Sharifi, Haiyong Xie, "Design and Implementation of Access Control as a Service for IaaS Cloud" in Scienceengineering.org ,2013, vol.2, no.3, pp. 115-130.

[10] Jan Kolter, Rolf Schillinger, Günther Pernul,"Building a Distributed Semantic-aware Security Architecture" in IFIP,2007,vol.232, pp 397-408.