IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 2, Ver. III (Mar-Apr. 2016), PP 114-117
www.iosrjournals.org

Improved Identity Based Encryption with Secured Revocation Mechanism in Cloud Computing

S.Dhivya[1], P.Senthil[2],
PG Scholar[1], Assistant Professor[2], Department of Information Technology[1,2],
Kongunadu College of Engineering and Technology[1,2], Tamilnadu.

Abstract: *Cloud data storing and retrieval is mostly important process in the cloud computing environment because of which cloud service providers are increase. When users attempts to store their contents in the third party service providers, the major challenge that might arise is the security. To ensure the security, data's are stored in the encrypted formats. Here the data access control would be more difficult problem where the data access needs to be limited for the available users. In this work, identity based encryption is used to limit the data access permission for the users by encrypting the data contents using the unique identity information. The identity based encryption is done in the block level to control the data contents that are provided to the users. To ensure the security from the malicious users, this work introduces the user revocation scheme. Revocation process is outsourced to the key update server to reduce the burden of private key generator. The overall burden of revoked users is eliminated by separating the key updation process from the data server. The key updation server is splitted and distributed to the different components such updation key generation process to the key updation server and the key updation process to the individual users. The experimental tests conducted by proved that the proposed methodology provides better result than the existing approach in terms of improved security level.*

I. Introduction

Cloud computing is a promising computing paradigm which recently has being drawn extensive attention from a both academia and industry. By combining a set of existing and new techniques from it research areas such as Service Oriented Architectures (SOA) and virtualizations, cloud computing is regarded as such a computing paradigms in which resources in the computing infrastructures are provided as services over the Internet[1]. Key distributions are done in a decentralized way. One limitation is that the cloud knows the access policy for each record stored in the cloud.

Data security, as it exists in many other applications, is among these challenges that would raise great concerns from user when they store sensitive information's on cloud server. Cloud computing multitenancy and virtualization futures posed unique securities and access control challenges due to sharing of physical resources among potential trusted tenants, resulting in an increased risk of side channel attacks [2]. Clouds can be classified as public, private or hybrid. Cloud computing realize on sharing of resources to achieve coherence and economies of scales, similar to a utility likes the electricity grid over a network. Data access control in the cloud leads to a security concern which provides a main research goal to the researchers and developer of cloud computing. The main goal of this project is to provide a privacy and security concern for the cloud storage data owner when they are outsourcing their confidential data [3].

Cloud infrastructures can roughly categorized as either private or public. In private clouds, the infrastructure is managed and owned by the customer and located on-premise means that access to customer data is under its control and is only granted to parties it trusts [4]. The addition of virtualized layers also means that accountability might require the identification not only of the virtual server in which an events takes place,, but also the physical server. Once cloud computing steps into our daily lives, any locally stored information, such as email, word processing documents and spreadsheets, could be remotely stored in a cloud. Secure provenance is of paramount importance to the flourish of cloud computing, yet it is still challenging today [5].

II. System Analysis

Existing System

It can be done by integrating the attributes with the encrypted plain text. The data will be encrypted under the access control scheme came from the attribute authority by using the symmetric key encryption algorithm.

Cloud storage is an important service of cloud computing, which offers services for a data owners to host their data in these cloud. This new paradigm of data hosting and data access service introduces a great challenge to a data access control. Because the cloud server cannot been fully trusted by a data owners, they can no longer relay on servers to do a access control. Cipher text Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in the cloud storage systems, because it gives the data ownership more direct control access policies. It can be done by a integrating the attributes with their encrypted plain text. The

data will be encrypted under the access control schemes came from the attribute authorities by using the symmetric key encryption algorithms.

Difficulties

In the existing works the symmetric encryptions is applied for the data encryption, where there may been possibility of data collision. That is there may be possibility of retrieving the entire contents of the files in the receiver side. The attribute attacker may act as an attacker, where there is a possibility of issuing a wrong secret key to the users which will prevent them from the accessing the data contents.

III. Proposed System

In the proposed work, outsourcing computation is introduced into Identity Based Encryption (IBE) revocation, and formalizes the security definition of outsourced revocable IBE for the first time to the best of our knowledge. It propose a scheme to offload all the key generation related operations during key-issuing and key update, leaving only a constant number of simple operations for Private Key Generator(PKG) and eligible users to perform locally. In this scheme, it realizes revocation through updating the private keys of the unrevoked users. But unlike traditional IBE which trivially concatenates time period with identity for key generation/update and requires to re-issue the whole private key for unrevoked users, it propose a novel collusion-resistant key issuing technique: It employ a hybrid private key for each user, in which a connector is involved to connect and bound two sub-components, namely the identity component and the time component. At first, user is able to obtain the identity component and a default time component (i.e., for current time period) from PKG as his/her private key in key-issuing. Afterwards, in order to maintain decryptability, unrevoked users needs to periodically request on key update for time component to a newly introduced entity named Key Update Cloud Service Provider (KU-CSP).

Machine Selection

CNC is computerized technology by controlling the relative movements between the tool and the work piece geometrical shapes are machined. Control of these relative movements through coded letters numbers is known as Numerical Control of machine tools.

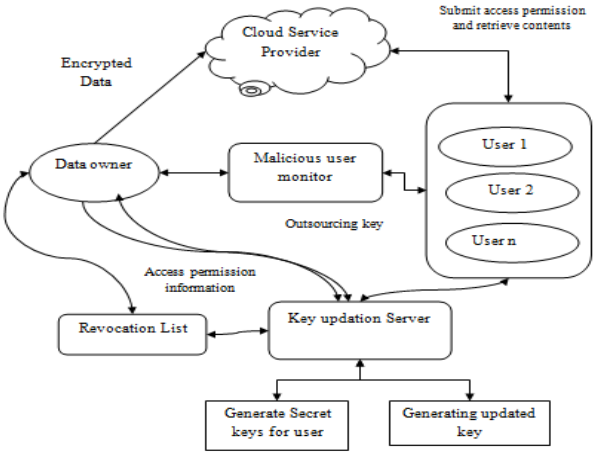

Fig.1 System Architecture

IV. Cloud Setup

The cloud network environment consists of the roles of user, data owner and the cloud server. The data owner is nothing but who stores and shares their health information. The data owner is responsible for encrypting and sharing the access control permission with the users. The cloud server is the one who is responsible for storing their contents into the network. The cloud server will store the contents received from the data owners and the authentication of valid users will be performed by the cloud servers.

Encryption and Decryption Phase

In this module, encryption process of original contents to be stored in the cloud storage that is done by the cloud data owners and the decryption process to be done by the cloud users are given.

To ensure the security of the cloud stored contents from them who are meant to be third party servers, cryptographic based encryption is introduced. This will allow users to store the encrypted contents in the cloud server instead of storing the plain texts directly. Thu the security for the cloud data owners is ensured.

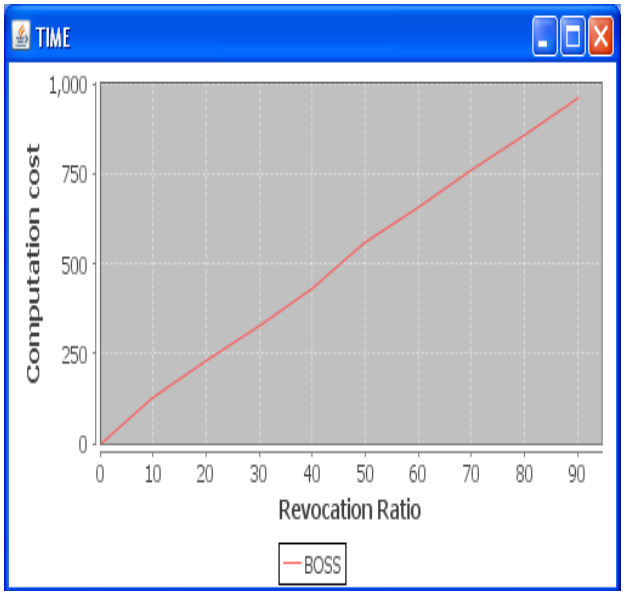

Fig.2 Computation overhead

Computation overhead is defined as the total processing complexity that is consumed for revoking the users who are involved in the system. Computation overhead of the proposed research scenario should be less for the improved system performance. The representation of the computation overhead which is obtained in the proposed research is depicted in the following graphical representation.

S.No	Revocation Ratio	Computation Overhead
1	10	120
2	20	240
3	30	300
4	40	460
5	50	580
6	60	670
7	70	750
8	80	860
9	90	980

Table.1 Computation Overhead Measures

V. Time Complexity Comparison

Time complexity is defined as the total time consumed for processing the user submitted query and the time taken revoke the users in the flexible manner. The time complexity is represented in the following graphical representation.

In this figure time complexity is depicted. In the x axis different revocation ratio is represented. In the y axis time complexity is represented. From this graph, it is proved that the time complexity of the proposed research scenario is increasing in the linear manner.

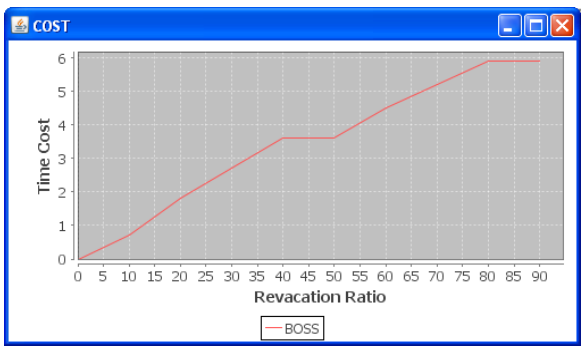

Figure.6.2Time Complexity Comparison

S.No	Revocation Ratio	Time Cost
1	10	0.8
2	20	1.85
3	30	2.7
4	40	3.6
5	50	3.6
6	60	4.5
7	70	5.2
8	80	5.95
9	90	5.95

Table.2 Time Cost Measures

VI. Results And Discussions

Cloud computing becomes most popular due to its flexibility of allowing multiple users to access the shared data. The data access control mechanism can be limited by the multiple attribute authorities by defining their individual attributes to control. In this work, identity based encryption with the consideration of the full anonymization is done with the consideration of the identity details of the users. This is proposed to provide an efficient access control over a third party providers and users with security concern. The malicious users and malicious providers cannot access the data's without knowing the privileged commitment message details. The experimental results prove that our proposed mechanism provides an efficient result than the existing methodologies.

In future malicious behaviour of the key updation server can be updated in terms of their malicious behaviour. The different encryption standards that are based on the different malicious users can be prevented by accessing the terminologies that denoted by the malicious key updation server. There is a revocation list to ensure that the users are revoked or not. It is used to secure the data content from malicious users.

Data integrity and confidentiality mechanisms can be integrated with these schemes to ensure the provisioning of the fresh copies of data contents to the other users. Data access control process can be decentralized to reduce the computation overhead that might get increased in the centralized server.

References

[1]. Allison Lewko1, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters(2010), "Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption", Advances in cryptology, Lecture Notes in Computer Science, Volume 6110, pp 62-91.

[2]. Brent Waters(2011), "Ciphertext-Policy Attribute-Based Encryption:An Expressive, E_cient, and Provably Secure Realization", Public key cryptography, Lecture Notes in Computer Science Volume 6571, pp 53-70.

[3]. Deepak Mishra, Manish Shrivastava(2012), "Optimal service pricing for cloud based services", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2.

[4]. HUANG Qinlong, MA Zhaofeng, YANG Yixian, NIU Xinxin, FU Jingyi(2014), "Attribute Based DRM Scheme with Dynamic UsageControl in Cloud Computing", China Communications, V olume:11 , Issue: 4, PP: 50 – 63.

[5]. Kai Hwang, Deyi Li(2010), "Trusted Cloud Computing with Secure Resources and Data Coloring", Internet Computing,Volume:14 Issue: 5, PP:14 – 22.

[6]. Kyle Chard, and Kris Bubendorfer (2013) "High Performance Resource AllocationStrategies for Computational Economies", IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 1.

[7]. Ming Li, Shucheng Yu, Yao Zheng,Kui Ren, and Wenjing Lou (2013), "Scalable and Secure Sharing of PersonalHealth Records in Cloud Computing UsingAttribute-Based Encryption", IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 1.

[8]. Sheng Di and Cho-Li Wang(2013), "Dynamic Optimization of Multi-AttributeResource Allocation in Self-Organizing Clouds", Parallel and Distributed Systems, IEEE Transactions on Volume: 24 , Issue: 3 , Page(s): 464 – 478.

[9]. Yao Wang, Julita Vassileva, "Trust and Reputation Model in Peer-to-Peer Networks", Proceedings of the 3rd International Conference on Peer-to-Peer Computing, Page 150, ISBN:0-7695-2023-5.

[10]. Zhiguo Wan, Jun'e Liu, and Robert H. Deng(2012), "HASBE: A Hierarchical Attribute-Based Solutionfor Flexible and Scalable Access Controlin Cloud Computing", IEEE Transactions On Information Forensics And Security, Vol. 7, No. 2.