Revocable Storage Identity Based Encryption and Sharing Information in Cloud

P. Ashok Kumar

Pg Scholar

Mr. POGAKU RAJ KUMAR

Assistant Professor

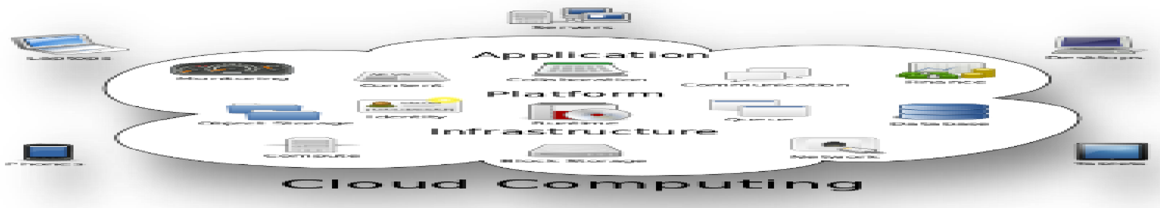
VAAGDEVI COLLEGE OF ENGINEERING, AUTONOMOUS, WARANGAL

Abstract- Cloud computing offers a flexible and convenient way to share data, which provides diverse benefits to society and people. But there is a natural resistance for users to directly outsource shared data to the cloud server because the data often contains valuable information. Therefore, it is necessary to place a cryptographically improved access control in the shared data. Identity-based encryption is a promising cryptographic primitive for building a convenient data exchange system. However, access control is not static. That is, when the authorization of certain users has expired, there must be a mechanism that can eliminate it from the system.

Therefore, the revoked user can not access the shared data previously and subsequently. To this end, we propose a concept called encryption based on the revocable storage identity (RS-IBE), which can provide forward / backward security of the encrypted text by simultaneously presenting the user's revocation and update characteristics. encrypted day In addition, we present a concrete RS-IBE construction and test its security in the defined security model. The performance comparisons indicate that the proposed RS-IBE system has advantages in terms of functionality and efficiency and that, therefore, it is possible to establish a practical and cost-effective data exchange system. Finally, we provide the results of the implementation of the proposed system to demonstrate its viability.

1 INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) provided as a service through a network (usually the Internet). The name comes from the common use of a symbol in the form of a cloud as an abstraction of the complex infrastructure contained in the diagrams of the system. Cloud computing provides remote services with the data, software and calculations of a user. Cloud computing is made up of hardware and software resources that are available on the Internet as services managed by third parties.



Structure of cloud computing

How Cloud Computing Works?

The goal of cloud computing is to apply traditional supercomputing or high-performance computing power, normally used by military and research facilities, to make tens of billions of calculations per second, in consumer-oriented applications, such as financial portfolios, to deliver personalized information, to provide data storage or to feed large and immersive computer games.

Cloud computing uses networks of large groups of servers that generally run low-cost consumer PC technology with specialized connections to distribute data processing tasks through them. This shared IT infrastructure contains large groups of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

Models of features and services:

The main characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are detailed below:

- Self-service on demand: a consumer can unilaterally supply computer capabilities, such as server time and network storage, as needed automatically without requiring human interaction with the provider of each service.
- Broad access to the network: the capacities are available through the network and accessed through standard mechanisms that

promote the use of heterogeneous thin or thick platforms (for example, mobile phones, laptops and PDAs).

- Collection of resources: the provider's computing resources are grouped to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of place independence, since the client usually has no control or knowledge about the exact location of the provided resources, but can specify the location at a higher level of abstraction (eg, country, state or data center).). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- Rapid elasticity: capabilities can be provisioned quickly and elastically, in some cases automatically, to quickly scale and launch quickly to scale quickly. For the consumer, the capacities available for provisioning often seem to be unlimited and can be purchased in any quantity at any time.
- Measured service: cloud systems automatically control and optimize the use of resources taking advantage of a measurement capacity at some level of abstraction appropriate for the type of service (for example, storage, processing, bandwidth and active user accounts)). The use of resources can be managed, controlled and reported, providing transparency for both the provider and the consumer of the service used.

Service models:

Cloud Computing comprises three different service models, namely, Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS). The three service models or layer are completed with an end-user layer that encapsulates the perspective of the end user in cloud services. The model is shown in the figure below. If a user in the cloud accesses services in the infrastructure layer, for example, they can run their own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance and security of these applications. If she accesses a service in the application layer, these tasks are usually handled by the cloud service provider.

Benefits of cloud computing:

1. Achieve economies of scale: increase production volume or productivity with fewer people. Your cost per unit, project or product plummets.

2. Reduce spending on technological infrastructure. Keep easy access to your information with a minimum initial expense.

Pay on the fly (weekly, quarterly or annual), according to the demand.

3. Globalize your workforce at a low price. People from all over the world can access the cloud, as long as they have an Internet connection.

4. Optimize the processes. Do more work in less time with fewer people.

5. Reduce capital costs. It is not necessary to spend a lot of money on hardware, software or license fees.

6. Improves accessibility. You have access anytime and anywhere, making your life much easier!

7. Monitor projects more effectively. Stay within budget

2 Related work

2.1 Revocable identity-based encryption

The concept of identity-based encryption was introduced by Shamir and conveniently instantiated by Boneh and Franklin. IBE eliminates the need to provide public key infrastructure (PKI). Regardless of the configuration of IBE or PKI, there must be an approach to revoke users of the system when necessary, for example, the authority of a user expires or the secret key of a user is revealed. In the traditional PKI environment, the problem of revocation has been well studied and several techniques are widely approved, such as the certificate revocation list or the validity periods added to certificates. However, there are only a few studies on revocation in the EIB environment. Boneh and Franklin first proposed a form of natural revocation for IBE. They added the current period to the encrypted text and the unrevoked users received periodic private keys for each period of the key authority. Unfortunately, this solution is not scalable because it requires the key authority to do a linear job on the number of unrevoked users. In addition, a secure channel is essential for the responsible authority and unrevoked users to pass new passwords. To overcome this problem, Boldyreva, Goyal and Kumar have introduced a new approach to achieve effective revocation. They used a binary tree to handle the identity so that their RIBE system reduces the complexity of revoking the logarithmic key (instead of linear) in the maximum number of users in the system. However, this system only provides selective security. Subsequently, using the aforementioned revocation technique, Libert and Vergnaud [have proposed a safe and adaptable RIBE scheme based on a variant of the IBE scheme of Water, Chen et al. builds a RIBE scheme from lattices. Recently, Seo and Emura proposed an effective RIBE

Realistic threat-resistant schema called decryption key exposure, which means that decryption key disclosure for the current time period has no effect on decryption key security for other periods of time. Inspired by previous work and, Liang et al. Introduces a re-encrypted proxy based cloud-based revocable identity that supports user revocation and encrypted text update. To reduce the complexity of the revocation, they used a transmission encryption scheme [2] to encrypt the encrypted text of the update key, independent of the users, so that only unrevoked users can decrypt the update key. up to date. However, this type of revocation method can not withstand the collusion of revoked users and unrevoked malicious users, since unrevoked malicious users can share the update key with revoked users. In addition, to update the encrypted text, the key authority in your system must maintain a table for each user to produce the re-encryption key for each period, which greatly increases the authority's workload. key.

3. PRELIMINARIES:

3.1. DECISIONAL BDHE ASSUMPTION:

The decision problem ℓ-BDHE is formalized in the following way. Select a group G 1 with priority p as a function of the safety parameter λ g select a generator G1 and a, s <- R ZP and f i = a i g. .T provide the vector f = (g, gs, f 1, ..., ℓ f, ℓ + f 2, ..., f 2ℓ) and an element D ∈ G 2 to a probabilistic polynomial time algorithm (PPT)) C, leave 0 to indicate that D = e (gs ga $ l $ + 1), and outputs 1 to indicate that D is a random element of g 2.

3.2. ALGORITHM KUNODES:

Using this algorithm only in the user revoked a period of time are they able to decipher the encrypted text

ENTRY: binary tree revocation list, point

OUTPUT: Subset product smaller nodes AND BT, so that Y contains an ancestor for each node that is not revoked before the period

DO NOT:

1. The owner of the data uploads the file to the cloud with the validity time

2. The data user accesses the data.

2.1. If the user tries to access the data within a specific time, he can access the data

2.2. Otherwise, the owner of the data must update the key.

3. The owner of the data updates the key used by the user.

4. Next, update the encrypted text. This will provide both forward and backward security for data stored in a cloud. DOI: 10.18535 / ijecs / v6i3.29 Sonia Jenifer Rayen**WORKING:**

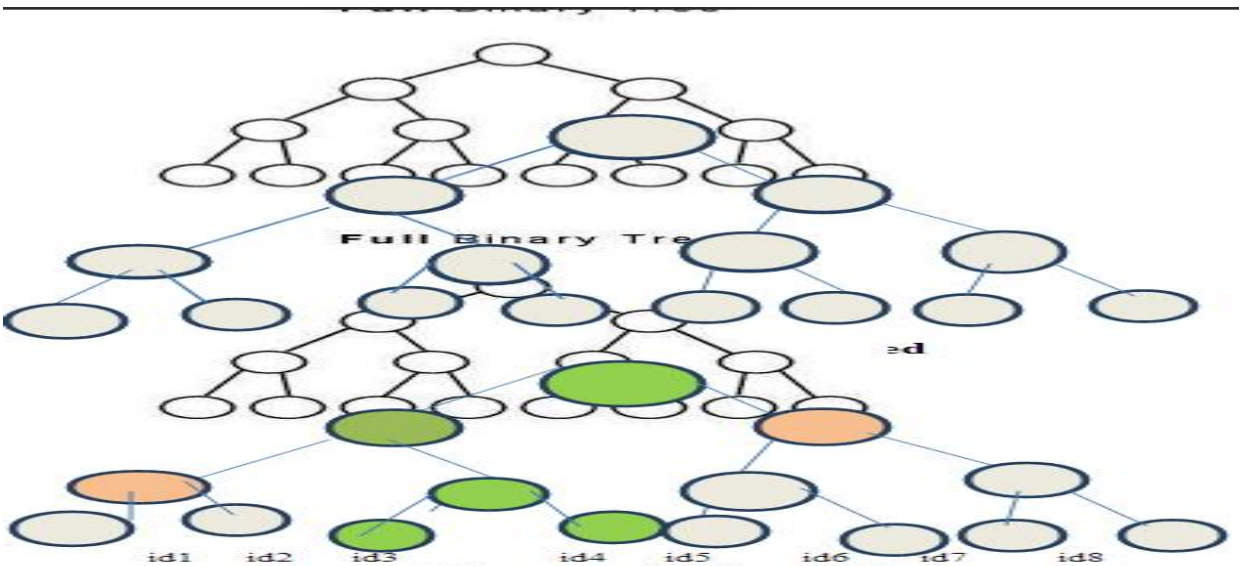


Fig :user id3 is revoked

By this algorithm ,when we rovoke the leaf node(id3) their ancestors also get updated(nod es in green color) and the node which shares the same key of revoked nod(nodes in orange color)e also get updated.

Algorithm 1

```
KUNodes( BT , RL, t)
X,Y←−∅
for all (ηi,ti)∈ RL do
    if ti≤t then
        Add Path(η i) to X
    end if
end for
for all θ ∈ X do
    if θ l ∈ /X then
        Add θ l to Y
    end if
    if θ r ∈ /X then
        Add θ r to Y
    end if
end for
if Y= ∅ then
    Add the root node ε to Y
end if
return Y
```

IV CONCLUSIONS

Cloud computing provides great convenience to people. In particular, it coincides perfectly with the greater need to share data on the Internet. In this article, to create a cost-effective data exchange and secure cloud computing system, we have proposed a concept called RS-OIE, which simultaneously supports the revocation of identification and update of encrypted text. as well as the data shared later. In addition, a concrete construction of RS-IBE is presented. The proposed RS-OIE scheme has been shown adaptive-safe in the standard model, under the assumption of ℓ DBHE intake. The results of the comparison show that our system has advantages in terms of efficiency and functionality, and therefore more feasible for practical applications is.

REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres and Mr. Lindner, "A break in the clouds towards a cloud definition" ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, 2008.

[2] iCloud. (2014) Apple storage service. [Online] Available: https://www.icloud.com/

[3] Azure. (2014) Azure Storage Service. [Online] Available: http://www.windowsazure.com/

[4] Amazon. (2014) Amazon simple storage service (amazon s3). [Online] Available: http://aws.amazon.com/s3/

[5] K. Chard, K. Bubendorfer, S. and O. F. Caton Rana, "Cloud computing social: a vision to share socially motivated resources", Services, IEEE Transactions on, vol. 5, no. 4, pp. 551-563, 2012.

[6] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public audit for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362-375, 2013.

[7] G. Anthes, "Security in the Cloud", Communications of the ACM, vol. 53, no. 11, pp. 16-18 of 2010.

[8] K. Yang and X. Jia, "Same dynamic efficient, and secure storage for data in the cloud", parallel and distributed systems, IEEE Transactions on, vol. 24, no. 9, pages 1717-1726, 2013.

[9] B. Wang, B. and H. Li Li, "public audit data shared with the effective elimination of users in the cloud", in INFOCOM, 2013 IEEE Proceedings. IEEE, 2013, pp. 2904-2912.

[10] S. Ruj, M. Stojmenovic and A. Nayak "decentralized access control with anonymous authentication data stored in the cloud," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384-394, 2014.

[11] X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "The exchange of authentic anonymous data and profitable with before, security" Computers, IEEE transactions, 2014, doi: 10.1109 / TC.2014.2315619.

[12] C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou and RH Deng, "cryptosystem key aggregates for scalable data sharing in cloud storage", parallel and distributed systems, IEEE Transactions on, vol.25, no.2, pp. 468-477, 2014.

[13] A. Shamir, "cryptographic systems based on identity and signature schemes", in Advances in cryptology. Springer, 1985, p. 47-53.

[14] D. Boneh and M. Franklin, "Encryption based on the identity of the Weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586-615, 2003.

[15] S. Micali, "efficient certificate revocation" Tech. Rep., 1996.

[16] W. Aiello, S. and R. Lodha Ostrovsky, "identity digital fast revocation," Advances in cryptology - CRYPTO 1998, Springer, 1998, p. 137-152.

[17] D. Naor, M. Naor and J. Lotspiech, "Withdrawal and tracingschemes for stateless recipients," in Advances in Cryptology - CRYPTO 2001, Springer, 2001, pp. 41-62.