Data Security by Encryption during cloud transactions

B.Swana Latha Assistant Professor in Department of Information Technology in Teegala Krisha Reddy Engineering college.Telangana
Ch.Manideep Sai UG Scholar in Department of Information Technology in Teegala Krisha Reddy Engineering college.Telangana
M.Ajay Reddy UG Scholar in Department of Information Technology in Teegala Krisha Reddy Engineering college.Telangana
V.Manipoorna UG Scholar in Department of Information Technology in Teegala Krisha Reddy Engineering college.Telangana

Abstract: Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the society and individuals. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the data often contain valuable information. Thus, it is necessary to place cryptographically enhanced access control on the shared data identity-based encryption is a promising cryptographical primitive to build a practical data sharing system. However, access control is not static. That is, when some user's authorization is expired, there should be a mechanism that can remove him/her from the system. Consequently, the revoked user cannot access both the previously and subsequently shared data. To this end, we propose a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of ciphertext by introducing the functionalities of user revocation and ciphertext update simultaneously. Furthermore, we present a concrete construction of RS-IBE, and prove its security in the defined security model. The performance comparisons indicate that the proposed RS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective
data-sharing system. Finally, we provide implementation results of the proposed scheme to demonstrate its practicability.

Terms—Cloud computing, data sharing, revocation, Identity-based encryption, ciphertext update, decryption key exposure.
.

I. INTRODUCTION

Cloud computing enables users to get intended services irrespective of time and location across multiple platforms (e.g., mobile devices, personal computers), and thus brings great convenience to cloud users. Among numerous services provided by cloud computing, cloud storage service, such as Apple's iCloud, Microsoft's Azure and Amazon's S3 [4], a more flexible and easy way to share data over the Internet, which provides various benefits for our society. However, it also suffers from several security threats, which are the primary of cloud users.

Security Goals:

- Data confidentiality
- Backward secrecy
- Forward secrecy

II. MOTIVATION

RIBE features a mechanism that enables a sender to append the current time period to the ciphertext such that the receiver can decrypt the ciphertext only under the condition that he/she is not revoked at that time period. A RIBE-based data sharing system works as follows:

Step 1: The data provider (e.g., `David`) first decides the users (e.g., `Alice` and `Bob`) who can share the data. , David encrypts the data under the identities `Alice` and `Bob`, and uploads the ciphertext of the shared data to the cloud server.

Step 2: When either `Alice` or `Bob` wants to get the shared data, she or he can download and decrypt the corresponding ciphertext. However, for an unauthorized user and the cloud server, the plaintext of the shared data is not available.

Step 3: In some cases, e.g., `Alice`'s authorization gets expired, `David` can download the ciphertext of the shared data, and then decrypt-then-re-encrypt the shared data such that `Alice` is prevented from accessing the plaintext of the shared data, and then upload the re-encrypted data to the cloud server again.

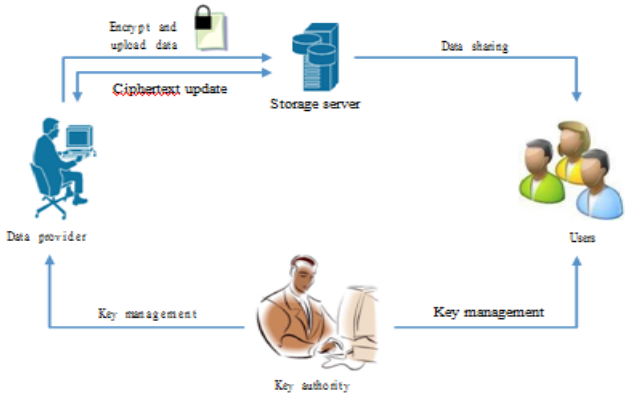

Figure-. A natural RIBE-based data sharing system

The data stored in the cloud may be frequently updated by the user ,including insertion ,deletion, modification, appending, recording etc, to ensure storage correctness under dynamic data update is hence of paramount importance. However solution to resolve data lost issue by back up with data storage on cloud or external server.

Obviously, such a data sharing system can provide con fidentiality and backward secrecy. Furthermore, the method of decrypting and re-encrypting all the shared data can en-sure forward secrecy. However, this brings new challenges. Note that the process of decrypt-then-re-encrypt necessarily involves users' secret key information, which makes the overall data sharing system vulnerable to new attacks. In general, the use of secret key should be limited to only usual decryption, and it is inadvisable to update the ciphertext periodically by using secret key.

In this paper, we introduce a notion called revocable-storage identity-based encryption (RS-IBE) for building a cost-effective data sharing system that fulfills the three security goals. More precisely, the following achievements are captured in this paper:

The benefits of cloud-based services have become almost cliché: universal accessibility, Web-based interfaces, reduced capital expenditures, reduced personnel costs and greater flexibility. client to spell out in advance how and when they can access backups, the provider's responsibilities in making sure the client can access your data when necessary and the client's access to backups if they decide to change providers. Regardless of any promises a cloud provider might make in their marketing materials. choose to use a cloud-based service to back up a wireless network, make sure you have protocols in place in case you want to do a bare-metal restore of a device on the network. In order to access a wireless network, the system will need at minimum an operating system and network drivers. It might be necessary to boot the system being restored using a thumb drive or USB stick in order to create an operating environment where a wireless connection to the cloud-based backup can occur. Cloud-based storage has become a commodity so providers might prefer to store your data as inexpensively as possible. As a result, the provider's data center might not be located physically within the US borders. If your backup data is subject to government or industry data security regulations, you need to ensure that the data centers where your backups are stored meet the appropriate requirements.

This duplicate data center, of course, comes with duplicate work. This may include at minimum: Facilities and real estate to house the IT infrastructure .Management and security personnel for these facilities. Enough server capacity to store all data and meet the scaling requirements of your applications. Support staff for maintaining the infrastructure. Internet connectivity with enough bandwidth to power your applications .Network infrastructure such as balancers firewalls, routers, switches, and load.

II. oBJECTIVE

a) Easily implemented with high reliability

Disaster recovery solutions are relatively easy to set up in the cloud, especially compared to setting up your own duplicate data center.

You don't have to purchase and deploy backup servers, drives, and disks. Rather, you can easily and instantly deploy a cloud storage solution such as Amazon S3 to back up your data, or even tier your backup with longer-term data storage solutions like Amazon Glacier to lower costs even more. And it's extremely easy to restore your infrastructure quickly if your app is backed up in the cloud. There's no more dealing with transportation and restoration of backup tapes to get your application up and running again. When using the cloud for DR, you can access all of your data through the internet much more quickly and easily.

Disaster recovery is just much easier in the cloud.

b) Scalability

Cloud services can be easily scaled up to meet demand as needed. In the traditional DR scenario, you had to make sure that you had enough server capacity in your duplicate data center to meet demand. And if you didn't, app performance would be slow and sluggish. With the cloud, scaling capacity is simple, quick, and more cost effective, ensuring that your customers will have a great user experience even in the case of a disaster.

A comprehensive disaster recovery plan will help you do so. And cloud computing can help you easily implement this plan to increase reliability and flexibility while saving time and money.

Cloud computing, based on virtualization, takes a very different approach to disaster recovery. With virtualization, the entire server, including the operating system, applications, patches and data is encapsulated into a single software bundle or virtual server. This entire virtual server can be copied or backed up to an offsite data center and spun up on a virtual host in a matter of minutes.

Since the virtual server is hardware independent, the operating system, applications, patches and data can be safely and accurately transferred from one data center to a second data center without the burden of reloading each component of the

server. This can dramatically reduce recovery times compared to conventional (non-virtualized) disaster recovery approaches where servers need to be loaded with the OS and application software and patched to the last configuration used in production before the data can be restored.

III. IMPLEMENTATION

The cloud shifts the disaster recovery tradeoff curve to the left, as shown below. With cloud computing (as represented by the red arrow), disaster recovery becomes much more cost-effective with significantly faster recovery times.

- We provide formal definitions for RS-IBE and its corresponding security model; We present a concrete construction of RS-IBE. The proposed scheme can provide confidentiality and backward/forward secrecy simultaneously; We prove the security of the proposed scheme in the standard model, under the decisional ℓ-Bilinear DiffieHellman Exponent (ℓ-BDHE) assumption. In addition, the proposed scheme can withstand decryption key exposure;

- **Algorithm 1**
- **Data node**(set,left,right)

1:n odes are set null both right and left.
2: **for all** edges to sub nodes with instances of null
3: **if** $null \leq t$ **then**
4: Add Path to solution set
5: **end if**
6: **end for**
7: **for all null edge each and nodes subset to the the total number of edges and nodes**
10: **end if**
11: **if every edge is connected to node then**
12: Add edge to optimal solution set
13: **end if**
14: **end for**
15: **if solution set** $= \emptyset$ **then**
16: Add the root node of graph to optimal set

17: **end if**18: **return** Y

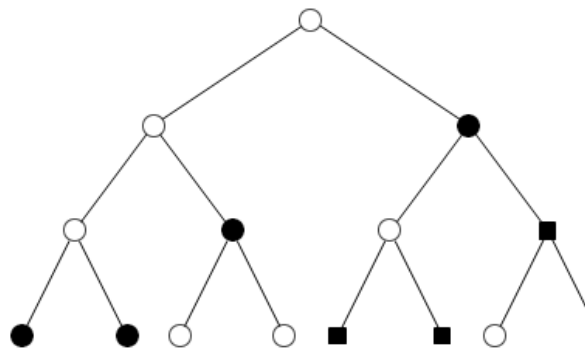

Figure:example of nodes in graph with centers.

IV. CONCLUSION

Cloud computing brings great convenience for people. Particularly, it perfectly matches the increased need of sharing data over the Internet. In this paper, to build a cost-effective and secure data sharing system in cloud computing, we proposed a notion called RS-IBE, which supports identity revocation and ciphertext update simultaneously such that a revoked user is prevented from accessing previously shared data, as well as subsequently shared data. Furthermore, a concrete construction of RS-IBE is presented. The proposed RS-IBE scheme is proved adaptive-secure in the standard model, under the decisional ℓ-DBHE assumption. The comparison results demonstrate that our scheme has advantages in terms of efficiency and functionality, and thus is more feasible for practical applications.

REFERENCES

[1] K.Yang, X.Jia, K.Ren, B.Zhang and R.Xie,"DAC-MACS: Effective data access control for multi authority cloud storage systems,"IEEE transactions on information Forensics & Security, vol. 7, 2012

[2]Ming Li,Shucheng Yu,Yao Zheng,Kui Ren,Wenjing Lou, "Scalable and secure sharing of personal heath records in cloud computing using attribute based encryption,"IEEE transactions on parallel and distributed systems, vol 24, 2013

[3]Elli Androulaki,Claudio Soriente,Luka malisa & Srdjan Capkun, "Enforcing location and time based access controlon cloud stored data,IEEE 34 th international conference on Distributed computing systems,2014.

[4]Baishuang Hu, Qin Liu,Xuhui Liu,Tao Peng,Guojun Wang & Jie wu, "DABKS:Dynamic attributebased Keyword search in cloud computing",IEEE communication and information systems security symposium,2017

[5]Quin Liu, Guojun Wang, & Jie wu,"Clock based proxy Re-encryption scheme in unreliable cloud,"IEEE 41st international conference on parallel processing workshops, 2012

[6]Kan Yang, he Liu, Xiao Hua jia, "Time domain attribute based access control for cloud based video content sharing: A cryptographic approach, IEEE transaction on Multimedia, vol 18, 2016

[7]Kui Ren, Cong Wang & Quian Wang, "Security Challenges for the Public Cloud, IEEE Computer Society, Jan2012

[8]Cong Wang, Quian Wang & Kui Ren, "Privacy preserving public auditing for data Storage Security in cloud Computing",IEEE communication society,2010.

[9]J.Bethencourt,A Sahai andb.Waters "cipher text Policy Attribute based encryption," In proceeding of the 28thIEEE symposium on security and privacy,IEEE 2007.

[10]R.L Rivest, A.Shamir and D.a Wagner,"Time lock puzzles and timed release Crypto,"Massachusets Institute of Technology, 1996

[11]Gartner Inc: Gartner identifies the Top 10 strategic technologies for 2011. Online. Available: . Accessed: 15-Jul-2011 http://www.gartner.com/it/page.jsp?id=1454221 Online. Available: . Accessed: 15-Jul-2011

[12] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N: Cloud Computing: A Statistics Aspect of Users. In First International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer Berlin; 2009:347–358.Google Scholar

[13] Zhang S, Zhang S, Chen X, Huo X: Cloud Computing Research and Development Trend. In Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China. Washington, DC, USA: IEEE Computer Society; 2010:93–97.View ArticleGoogle Scholar

[14] Cloud Security Alliance: Security guidance for critical areas of focus in Cloud Computing V3.0.. 2011. Available:

[15] Marinos A, Briscoe G: Community Cloud Computing. In 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer-Verlag Berlin; 2009.Google Scholar

[16] Giuseppe Pirr´o, Paolo Trunfio ,Domenico Talia, Paolo Missier andCarole Goble, 2010, "ERGOT: A Semantic-based System for Service Discovery in Distributed Infrastructures," 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing.

[17]VijaykumarJavaraiah Brocade Advanced Networks and Telecommunication Systems (ANTS), 2011, "Backup for Cloud and Disaster Recovery for Consumers and SMBs," IEEE 5th International Conference, 2011.

[18]Lili Sun, Jianwei An, Yang Yang, Ming Zeng, 2011, "Recovery Strategies for Service Composition in Dynamic Network,"
International Conference on Cloud and Service Computing.

[19]Xi Zhou, Junshuai Shi, YingxiaoXu, Yinsheng Li and Weiwei Sun, 2008, "A backup restoration algorithm of service composition in MANETs," Communication Technology ICCT 11th IEEE International Conference, pp. 588-591.

[20]Ms..KrutiSharma,ProfK.R.Singh, 2012, "Online data Backup And Disaster Recovery techniques in cloud computing:A review", JEIT, Vol.2, Issue 5.

[21]Y.Ueno, N.Miyaho, and S.Suzuki, , 2009, "Disaster Recovery Mechanism using Widely Distributed Networking and Secure Metadata Handling Technology", Proceedings of the 4th edition of the UPGRADE-CN workshop, pp. 45-48.

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

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

[24]Azure. (2014) Azure storage service. [Online]. Available: http://www.windowsazure.com/

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

[25]K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," *Services Computing, IEEE Transactions*.
C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," *Computers, IEEE Transactions on*, vol. 62, no. 2, pp. 362–375, 2013.
[26]G. Anthes, "Security in the cloud," *Communications of the ACM*, vol. 53, no. 11, pp. 16–18, 2010.
[27]K. Yang and X. Jia, "An efficient and secure dynamic auditing pro- tocol for data storage in cloud computing," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 24, no. 9, pp. 1717–1726, 2013.