

REVOCABLE-STORAGE INTEGRITY-BASED ENCRYPTION SECURE DATA SHARING IN CLOUD COMPUTING

Polampally Ashwini¹, Prof. D. Anji Reddy²

1. M.Tech Scholar, Department of CSE, Vaageswari College of Engineering, Karimnagar, Telangana, India– ashwinipolampally@gmail.com, 9059585923
2. Associate Professor, Department of CSE, Vaageswari College of Engineering, Karimnagar, Telangana, India-anjireddy.knr@gmail.com, 9618880999

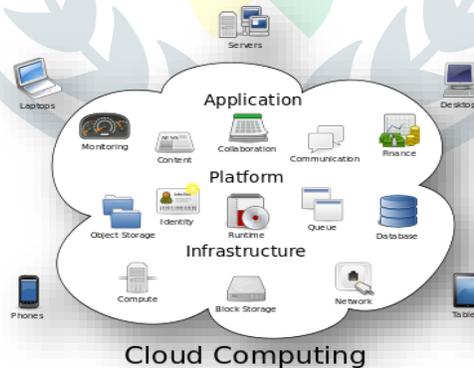
ABSTRACT:

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.

1. INTRODUCTION:

What is cloud computing?

Cloud computing is resources (hardware and software) that are delivered (typically the Internet). The common use of a cloud-abstraction for the complex system diagrams. Cloud services with a user's data, Cloud computing consists resources made available on party services. These services typically provide access to advanced software applications and high-end networks of server computers.



the use of computing software) that are delivered (typically the Internet). The common use of a cloud-abstraction for the complex system diagrams. Cloud services with a user's data, Cloud computing consists resources made available on party services. These

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 perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

Characteristics and Services Models:

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

- **On-demand self-service:** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- **Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling:** The provider's computing resources are pooled 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 location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid elasticity:** Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- **Measured service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Services Models:

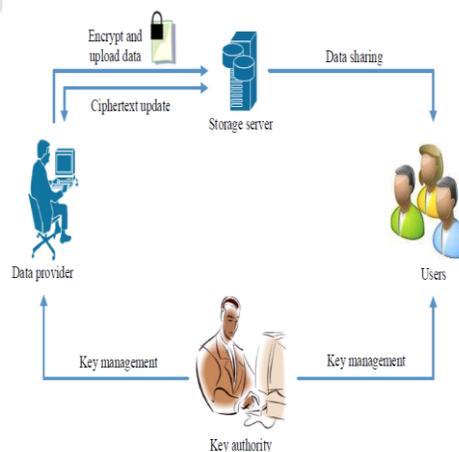
Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model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

Benefits of cloud computing:

1. **Achieve economies of scale** – increase volume output or productivity with fewer people. Your cost per unit, project or product plummets.
2. **Reduce spending on technology infrastructure.** Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.
3. **Globalize your workforce on the cheap.** People worldwide can access the cloud, provided they have an Internet connection.
4. **Streamline processes.** Get more work done in less time with less people.
5. **Reduce capital costs.** There's no need to spend big money on hardware, software or licensing fees.
6. **Improve accessibility.** You have access anytime, anywhere, making your life so much easier!
7. **Monitor projects more effectively.** Stay within budget and ahead of completion cycle times.
8. **Less personnel training is needed.** It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.
9. **Minimize licensing new software.** Stretch and grow without the need to buy expensive software licenses or programs.
10. **Improve flexibility.** You can change direction without serious “people” or “financial” issues at stake.

Advantages:

1. **Price:** Pay for only the resources used.
2. **Security:** Cloud instances are isolated in the network from other instances for improved security.
3. **Performance:** Instances can be added instantly for improved performance. Clients have access to the total resources of the Cloud's core hardware.
4. **Scalability:** Auto-deploy cloud instances when needed.
5. **Uptime:** Uses multiple servers for maximum redundancies. In case of server failure, instances can be automatically created on another server.
6. **Control:** Able to login from any location. Server snapshot and a software library lets you deploy custom instances.
7. **Traffic:** Deals with spike in traffic with quick deployment of additional instances to handle the load.

II.SYSTEM ARCHITECTURE:

III. EXISTING SYSTEM:

- ❖ Boneh and Franklin first proposed a natural revocation way for IBE. They appended the current time period to the ciphertext, and non-revoked users periodically received private keys for each time period from the key authority.
- ❖ Boldyreva, Goyal and Kumar introduced a novel approach to achieve efficient revocation. They used a binary tree to manage identity such that their RIBE scheme reduces the complexity of key revocation to logarithmic (instead of linear) in the maximum number of system users.
- ❖ Subsequently, by using the aforementioned revocation technique, Libert and Vergnaud proposed an adaptively secure RIBE scheme based on a variant of Water's IBE scheme.
- ❖ Chen et al. constructed a RIBE scheme from lattices.

Disadvantages of Existing System:

- ❖ Unfortunately, existing solution is not scalable, since it requires the key authority to perform linear work in the number of non-revoked users. In addition, a secure channel is essential for the key authority and non-revoked users to transmit new keys.
- ❖ However, existing scheme only achieves selective security.
- ❖ This kind of revocation method cannot resist the collusion of revoked users and malicious non-revoked users as malicious non-revoked users can share the update key with those revoked users.
- ❖ Furthermore, to update the ciphertext, the key authority in their scheme needs to maintain a table for each user to produce the re-encryption key for each time period, which significantly increases the key authority's workload.

IV. PROPOSED SYSTEM:

- ❖ It seems that the concept of revocable identity-based encryption (RIBE) might be a promising approach that fulfills the aforementioned security requirements for data sharing.
- ❖ 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. Then, 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.

Advantages of Proposed System:

- ❖ 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/forward² secrecy simultaneously
- ❖ We prove the security of the proposed scheme in the standard model, under the decisional ℓ -Bilinear Diffie-Hellman Exponent (ℓ -BDHE) assumption. In addition, the proposed scheme can withstand decryption key exposure
- ❖ The procedure of ciphertext update only needs *public information*. Note that no previous identity-based encryption schemes in the literature can provide this feature;
- ❖ The additional computation and storage complexity, which are brought in by the forward secrecy, is all upper bounded by $O(\log(T)^2)$, where T is the total number of time periods.

V.IMPLEMENTATION:

Modules:

- ❖ System Construction Module
- ❖ Data Provider
- ❖ Cloud User
- ❖ Key Authority (Auditor)

Modules Description:

System Construction Module

In the first module, we develop the proposed system with the required entities for the evaluation of the proposed model. The data provider (e.g., David) first decides the users (e.g., Alice and Bob) who can share the data. Then, David encrypts the data under the identities Alice and Bob, and uploads the ciphertext of the shared data to the cloud server.

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.

Data Provider

In this module, we develop the Data Provider module. The data provider module is developed such that the new users will Signup initially and then Login for authentication. The data provider module provides the option of uploading the file to the Cloud Server. The process of File Uploading to the cloud Server is undergone with Identity-based encryption format. Data Provider will check the progress status of the file upload by him/her. Data Provider provided with the features of Revocation and Ciphertext update the file. Once after completion of the process, the Data Provider logout the session.

Cloud User

In this module, we develop the Cloud User module. The Cloud user module is developed such that the new users will Signup initially and then Login for authentication. The Cloud user is provided with the option of file search. Then cloud user feature is added up for send the Request to Auditor for the File access. After getting decrypt key from the Auditor, he/she can access to the File. The cloud user is also enabled to download the File. After completion of the process, the user logout the session.

Key Authority (Auditor)

Auditor Will Login on the Auditor's page. He/she will check the pending requests of any of the above person. After accepting the request from the above person, he/she will generate master key for encrypt and Secret key for decrypt. After the complete process, the Auditor logout the session.

VI.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

VII. REFERENCES

- [1] 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.
- [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. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," *Services Computing, IEEE Transactions on*, vol. 5, no. 4, pp. 551–563, 2012.
- [6] 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.
- [7] G. Anthes, "Security in the cloud," *Communications of the ACM*, vol. 53, no. 11, pp. 16–18, 2010.
- [8] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 24, no. 9, pp. 1717–1726, 2013.
- [9] B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in *INFOCOM, 2013 Proceedings IEEE*. IEEE, 2013, pp. 2904–2912.
- [10] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," *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, "Cost-effective authentic and anonymous data sharing with forward security," *Computers, IEEE Transactions on*, 2014, doi: 10.1109/TC.2014.2315619.
- [12] C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem 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, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology*. Springer, 1985, pp. 47–53.
- [14] D. Boneh and M. Franklin, "Identity-based encryption from 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. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in *Advances in Cryptology–CRYPTO 1998*. Springer, 1998, pp. 137–152.
- [17] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in *Advances in Cryptology–CRYPTO 2001*. Springer, 2001, pp. 41–62.
- [18] C. Gentry, "Certificate-based encryption and the certificate revocation problem," in *Advances in Cryptology–EUROCRYPT 2003*. Springer, 2003, pp. 272–293.
- [19] V. Goyal, "Certificate revocation using fine grained certificate space partitioning," in *Financial Cryptography and Data Security*. Springer, 2007, pp. 247–259.
- [20] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proceedings of the 15th ACM conference on Computer and communications security*. ACM, 2008, pp. 417–426.
- [21] B. Libert and D. Vergnaud, "Adaptive-id secure revocable identity based encryption," in *Topics in Cryptology–CT-RSA 2009*. Springer, 2009, pp. 1–15.
- [22] —, "Towards black-box accountable authority ibe with short ciphertexts and private keys," in *Public Key Cryptography–PKC 2009*. Springer, 2009, pp. 235–255.
- [23] J. Chen, H. W. Lim, S. Ling, H. Wang, and K. Nguyen, "Revocable identity-based encryption from lattices," in *Information Security and Privacy*. Springer, 2012, pp. 390–403.
- [24] J. H. Seo and K. Emura, "Revocable identity-based encryption revisited: Security model and construction," in *Public-Key Cryptography–PKC 2013*. Springer, 2013, pp. 216–234.