IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 6, June 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206099 |

Reliable Data Sharing Using Revocable Storage Identity-Based Encryption in Cloud Storage

Mr. M.Sivaganesh[1], J. Vidhyasri[2]

[1]Assistant Professor, Department of Computer Science and Engineering, Paavai Engineering College, Pachal, Namakkal, Tamil Nadu, India

[2] M.E CSE II[nd] Year, Department of Computer Science and Engineering, Paavai Engineering College, Pachal, Namakkal, Tamil Nadu, India

ABSTRACT : Security has always been concern when it comes to data sharing in cloud computing. Cloud computing provides high computation power and memory. Cloud computing is convenient way for data sharing. But users may sometime needs to outsourced the shared data to cloud server though it contains valuable and sensitive information. Thus it is necessary to provide cryptographically enhanced access control for data sharing system. This paper discuss about the promising access control for data sharing in cloud which is identity-based encryption. We introduce the efficient revocation scheme for the system which is revocable-storage identity-based encryption scheme. It provides both forward and backward security of ciphertext. Then we will have glance at the architecture and steps involved in identity-based encryption. Finally we propose system that provides secure file sharing system using identity-based encryption scheme.

KEYWORDS*:* Cloud computing; data sharing; revocation; identity-based encryption; security.

I. INTRODUCTION

Cloud service providers provides high computational capability and huge memory space at low cost. It gives users to access various services irrespective of time and location across various platforms. Cloud computing brings great convenience for users. Cloud services providers offer efficient way to share data over internet which provides various benefits to users. Various organizations prefer to use cloud storage for the data sharing because of high memory space and computational capability at low cost. User may need to outsourced data to cloud service provider. This outsourced data may contain valuable and sensitive information. Outsourced data is completely out control of users. Security is a primary concern of user when it comes to cloud storage for data sharing. Cloud storages are vulnerable to various attacks. Some cloud service providers uses third-party data centers which can also be victim of attacks. In the worst case cloud service providers may reveal data to public for illegal profit. In the data sharing system if the authorization of user is revoked, he/she should not be able to access data that was previously encrypted under his/her private key. While outsourcing shared data to cloud, users should control access to the shared data so that only authorized users can access shared data. Data confidentiality, authenticity, data availability, backward security, forward secrecy are the important security goals that secure data sharing system should provide. Data confidentiality means that unauthorized users should not be allowed to access plaintext of the shared data even cloud service providers also be deterred to access plaintext of shared data. Backward secrecy means that, if user's secret key is compromised or his/her authorization is expired, he/she should not be able to access the plaintext of the subsequently shared data that was earlier encrypted under his/her identity. Forward secrecy means that, if user's secret key is compromised or authorization is expired, he/she should not be able to access the plaintext of shared data that was previously accessed by him/her. Identity-based encryption is access control scheme which provides solution to all aforementioned problems and meets the aforementioned security goals. Exposure of the secret key is a greatest threat against the security of a revocable identity-based encryption scheme. It may be due to compromise of the security of the system or storing of the key at the machine.

The danger of successful cryptanalysis of the signature scheme itself is as big as the danger of key exposure, as long as we use well-known schemes and use large security parameters. The most widely considered solution to the

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

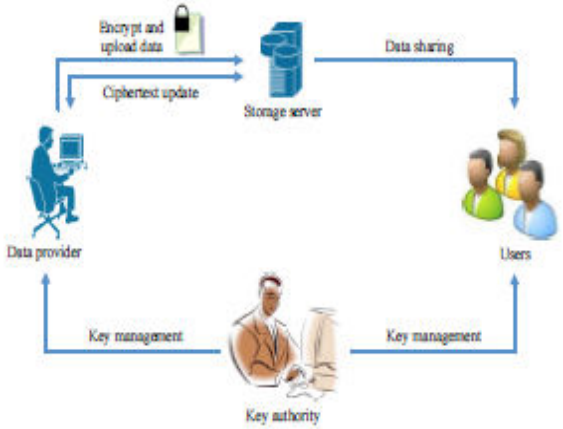
|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206099 |

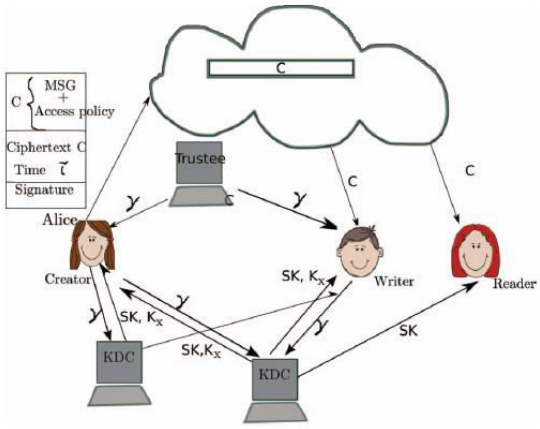
problem of key exposure is distribution of the key across multiple servers via secret sharing. Therefore we need to share the identity keys and secret keys to users using secure channel.

REVOCABLE IDENTITY-BASED ENCRYPTION.

Some unique information or attribute about the identity of the user (e.g. a user's email id). Identity-based encryption is a type of public-key encryption in which sender who has access to public parameters of the system can encrypt message using receivers email id or name as a key. The receiver will obtain decryption key from central authority, which is a trusted party that generates secret keys for users. Identity-based encryption (IBE) removes the need of Public Key Infrastructure (PKI). In this scheme the sender does not need to get the public keys and the certificates of the receiver for the encryption, the identities like name, email id together with common public attributes are used for encryption. The private keys are generated by trusted third party like private key generator (PKG). Identity-based encryption scheme can be used to secure the outsourced data available on cloud storage. The outsourced data is out control of the users and may contain the sensitive and valuable information. Revocation can be implemented as users' authorization expires he/she should not be access data previously shared to him/her.



NATURAL RIBE FRAMEWORK



SECURE CLOUD STORAGE FRAMEWORK. RELATED WORK

The idea of identity-based cryptography was introduced in 1984 by Shamir. But it was conveniently instantiated by Boneh and Franklin in 2001, building on the progress in elliptic curves with bilinear pairings. A first scheme for IBE was based on the bilinear Diffie-Hellman assumption in the random oracle model by Boneh and Franklin. In IBE schemes private key generator is essential for creating private keys for all users and because of that it is performance bottleneck for organization with large number of users.

Revocation capability is important for IBE as well as PKI setting. If the authority of some user is expired or the secret key is compromised there must be an approach to revoke user from the system. In the traditional PKI setting, the revocation problem has been well studied and various techniques are widely approved, such as appending validity periods to certificates or certificate revocation list. But there are only few studies on the revocation in identity-based encryption scheme. First natural revocation way for Identity based Encryption was proposed by Boneh and Franklin. They concatenated the current time period to the ciphertext and non revoked users received private keys from the key

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206099 |

authority periodically. But such solution was not scalable as it required the key authority to perform linear work in the number of nonrevoked users. In addition, a secure channel is required between key authority and non-revoked users to transfer new generated keys. To overcome this problem, Boldyreva, Goyal and Kumar introduced a novel approach for the efficient revocation. The reduce the complexity of Revocable Identity based encryption scheme to logarithmic in the maximum number of users by using binary tree to manage identity. Later by using the above revocation technique, Libert and Vergnaud proposed an adaptively secure Revocable Identity-based scheme based on variation of Water's IBE scheme, Chen et al. created RIBE scheme from lattices. Seo and Emura proposed an effective RIBE scheme which was resistant to decryption key exposure problem, that means though decryption key for current time period exposed would not have effect on the security of decryption keys for other time periods. Later Liang et al. [18] introduced a cloud based RIBE proxy re-encryption that allows user revocation and ciphertext update. They utilized a broadcast encryption scheme to encrypt the ciphertext of the update key, which is independent of users, such that only non-revoked users can decrypt the update key it also reduce the complexity of revocation. But this revocation method cannot oppose 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 needs to maintain a table for users to produce the re-encryption key for each time period which increases the workload of key authority.

PROPOSED SYSTEM

Our proposed system uses meta-data file technique to improve the security of file storage on cloud with implementation of identity-based encryption scheme. Our main motto is to provide secure cloud storage system with the help of RIBE (Revocable identity-based encryption). If user left the system his authorization should be revoked so that he/she should not be able to access files encrypted under his/her keys. Revocation can be implemented using meta-data file technique in our system.

We are storing meta-data file along with actual encrypted file having all the identification keys of users allowed to share file. We will remove his/her identity keys from all the meta-data files and re-encrypt all the files in the system after revocation of user. In our proposed system we define four modules cloud storage administrative control, user management, revocable identity based encryption and periodic key management. These modules implementation explained below.

ADVANTAGES.

One of the major advantages of any identity-based encryption scheme is that if there are only a finite number of users, after all users have been issued with keys the third party's secret can be destroyed. Our solution has several advantages. First, it provides secrecy for encrypted data which are stored in public servers. Second, it offers controlled data access and sharing among users, so that unauthorized users or untrusted servers cannot access or search over data without client's authorization.

That is, every client acts as a PKG by computing an ID-based pair of keys to encrypt the data that he intends to store in the cloud. As such, the data access is managed by the data owner. Second, by using a per data ID-based key, we provide a flexible sharing approach.

SYSTEM ARCHITECTURE

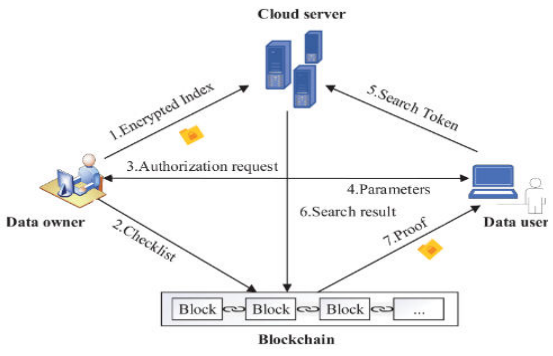


Fig.1.1 System Architecture

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206099 |

IMPLEMENTATION.

Cloud encryption solutions use two different methods to encrypt and decrypt data: symmetric and asymmetric. Data encryption for information stored on the cloud network ensures that even if the data is lost, stolen or mistakenly shared, the contents are virtually useless without the encryption key. Again, keys are only made available to authorized users. Identity-based encryption is a type of public-key encryption in which a user can generate a public key from a known unique identifier such as an email address), and a trusted third-party server calculates the corresponding private key from the public key.

TESTING

The project's implementation phase is where the theoretical design becomes a functional system. This is the last and significant stage in the framework life cycle. It is really the most common way of changing over the new framework into a functional one. Cloud Testing refers to the verification of software quality on a real-device cloud. QA teams can access thousands of real desktop and mobile devices for testing websites and apps in real time. Since these devices are hosted on cloud-based servers, they're accessible online at all times.

UNIT TESTING.

The set of tests performed by a single programmer prior to the unit's integration into a larger system is known as unit testing. Tests are performed on the module interface to guarantee that data properly enters and exits the program unit. The local data structure is looked at to make sure that temporarily stored data stays the same at every step of an algorithm's execution. The module is tested under boundary conditions to ensure that it functions properly within limits imposed to limit or restrict processing.

BLOCK BOX TESTING.

Black-box testing is a method of software testing that looks at an application's functionality without looking inside to see how it works or how it was built. Virtually every level of software testing can be tested using this method. Black box testing involves testing a system with no prior knowledge of its internal workings. A tester provides an input, and observes the output generated by the system under test.

II. CONCLUSION

The above schemes if applied to cloud computing can increase the security of the cloud storage. Identity-based encryption scheme can give access control to the user hand though the data is outsourced to the cloud servers. Revocable- Identity based encryption can prevent the shared data be accessed by revoked users from the system. In this proposed system techniques like meta-data file technique as well as periodic key management technique has been used to improve the security of the system.

It will help to reduce the computational cost of the system. 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] Jianghong Wei, Wenfen Liu, Xuexian Hu, "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption", IEEE Transactions on Cloud Computing, Vol. 14, No. 8, August 2015

[2] 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.

[3] 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.

[4] 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.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206099 |

[5] C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Keyaggregate cryptosystem for scalable data sharing in cloud storage," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 468–477, 2014. 2168-7161

[6] A. Shamir, "Identity-based cryptosystems and signature schemes," in
Advances In cryptology. Springer, 1985, pp. 47–53.

[7] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, 2003.

[8] S. Micali, "Efficient certificate revocation," Tech. Rep., 1996.

[9] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology–CRYPTO 1998. Springer, 1998, pp. 137–152.

[10] 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.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details