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 11, Issue 6, June 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

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: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106230 |

Performance and Security Analyses in Cloud Storage Using Ciphertext Poling Attribute Base Encryption

Chhaya Nayak

Assistant Professor, Department of Computer Engineering, Bhvarabai Sawant Institute of Technology & Research Wagholi , Pune, India

ABSTRACT: With the recent advancement in technology Cloud Computing has become an important paradigm that has attracted many users. Many people use the cloud every day without knowing its technology .Attribute-based encryption (ABE) is considered a promising technique for cloud storage where multiple users can access the same file. It plays a fundamental role in generating a public key for encrypting data and control user access policy. Cipher text policy attribute-based encoding (CP-ABE) allows knowledge house owners to outline their own access policies over user attributes and enforce the policies on the information to be distributed. In this paper, we propose an attribute-based access control scheme for data sharing in cloud storage system. Through proposed system the key written agreement drawback may well be solved by escrow-free key supplying protocol that is made using the secure two-party computation between the key generation centre and also the data-storing centre

KEYWORDS: Data sharing, attribute-based encryption, revocation, access control, removing escrow, Cloud Computing

I. INTRODUCTION

Following criteria must be fulfill first to achieve an effective, scalable and privacy-preserving data sharing service in cloud environment, the data owners who wants to share their data should be able to assign other cloud users with different access privileges to their data; secondly, the cloud environment needs to be support dynamic requests from the users so that data owners can add or revoke access privileges to other users by allowing them to create or delete their own data; finally, in cloud the user's privacy must be protected so that they can hide their private information while accessing the cloud.

Cloud storage is one of the most important feature provided by cloud computing. Currently it is being utilized as core component by various online platforms. Data sharing is one of the most important functionality of cloud storage. It enables multiple users to easily share their data with others by uploading their private data into the cloud storage, and rely on the cloud servers to provide data access control. With the development of the web and also the distributed computing technology, there is an increasing demand for knowledge sharing and process in an open distributed computing atmosphere. Recent development of the network and computing technology enables many of us to simply share their knowledge with others through on-line external storages.

Cloud Storage is a service which is offered by cloud with the facilities of storing, maintaining, managing, and backed up user's data over a network, which is usually the internet. Cloud Storage allows its user to store files so that the authenticate user can access them anytime from any location through the internet.

As we know that the traditional method of encryption like symmetric and asymmetric key encryption provides only the privacy, but not the access control mechanism.

The Attribute Based Encryption (ABE) is a public key cryptographic technique [8] through which can achieve both privacy and access control by secure data sharing among multiple users. Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent. In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. The ABE is mainly classified into two types, Key Policy Attribute Based Encryption (KP-ABE) and Cipher Policy Attribute Based Encryption (CP-ABE)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106230 |

Cipher text Policy Attribute-Based Encryption (CP-ABE) comes under asymmetric encryption is a growing research area that provides more and more interest from lots of researchers. CP-ABE more supports to the cloud based data sharing system and enables fine-grained access control over encrypted data. CP-ABE gives the more direct control on access policies and does not require the data owner to manage keys.

Key-policy attribute-based encryption (KP-ABE) is an important class of ABE, where cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. Key-policy attribute-based encryption (KP-ABE) is the cryptographic primitive which enables fine grained access control while still providing end-to-end encryption.

II. RELATED WORK

Firstly Sahai and Waters proposed an approach for Attribute-based encryption (ABE) [12] for one-to-many encryption in which users who fulfil certain requirements ciphertexts are encrypted for those. The most suitable variant for finegrained access control in the cloud environment is called ciphertext-policy (CP-)ABE, in which ciphertexts are associated with access policies, determined by the encrypt or and attributes describe the user, accordingly attributes are embedded in the users' secret keys. A ciphertext can be decrypted by someone if and only if, his attributes satisfy the access structure given in the ciphertext, thus data sharing is possible without prior knowledge of who will be the receiver preserving the flexibility of the cloud even after encryption.

Data owners demand high levels of security and confidentiality when they outsource their data to a cloud; although they usually encrypt their data when storing it in a cloud server, they still want control over it [16].
ABE mainly consist of two variations known as key-policy ABE (KP-ABE) and cipher text-policy ABE (CP- ABE). In KP-ABE, attributes are used to describe the encrypted information and policies are inbuilt in users keys while in CP-ABE scheme, in which the encryptor must decide who should or should not have access to the data that she encrypts, in other words we can say that cipher text are associated with policies, and users' keys are associated with sets of descriptive attributes. CP- ABE is a lot of acceptable to the information sharing system as a result of it puts the access policy selections within the hands of the information owners.
Based on the application scenarios of KP-ABE and CPABE, [17] proposed a PHR system framework that combines KP-ABE and CP-ABE together. In the framework, users are divided into personal domains (PSDs) and public domains (PUDs) according to their roles.

Replacement public key primitive known as Attribute-based cryptography (ABE). ABE has important advantage over the standard PKC primitives because it achieves flexible one-to-many cryptography rather than one-to-one. ABE is visualized as an important tool for addressing the problem of secure and fine-grained knowledge sharing and access management. In an ABE system, a user is known by a collection of attributes. Attribute-based cryptography (ABE) may be a promising cryptographic approach that achieves a fine-grained knowledge access management [4], [5], [6], [7]. It provides some way of defining access policies supported completely different attributes of the requester, environment, or the information object. Especially, cipher text policy attribute-based cryptography (CP-ABE) enables an encryption to outline the attribute set over a universe of attributes that a descriptor has to possess so as to decrypt the cipher text, and enforce it on the contents [6]. Thus, every user with a completely different set of attributes is allowed to decrypt different items of information per the security policy. This effectively eliminates the requirement to accept the data storage server for preventing unauthorized data access, which is that the traditional access management approach of like the reference monitor. Traditionally, this kind of communicative access management is implemented by using a trusty server to store knowledge locally. The server is entrusted as a reference monitor that checks that a user presents proper certification before permitting him to access records or files. However, services are progressively storing knowledge in a distributed fashion across many servers. Replicating knowledge across many locations has blessings in each performance and responsibility. The disadvantage of this trend is that it is progressively difficult to ensure the safety of knowledge using traditional methods; once data is hold on at many locations, the possibilities that one of them has been compromised will increase dramatically. For these reasons we would prefer to need that sensitive knowledge is stored in an encrypted kind so it will stay private even if a server is compromised. Fashionable distributed information systems need flexible access management models that transcend discretionary, necessary and

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

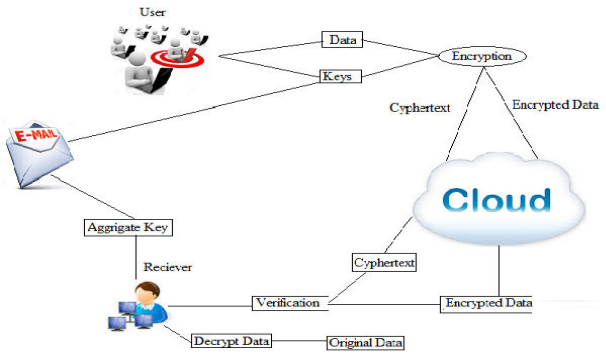
| DOI:10.15680/IJIRSET.2022.1106230 |

role-based access management. Recently planned models, like attribute-based access management, outline access management policies supported completely different attributes of the requester, surroundings, or the information object. On the opposite hand, the present trend of service-based info systems and storage outsourcing need increased protection of information together with access management strategies that are cryptographically enforced. The concept of Attribute-Based Encryption (ABE) fulfils the same requirements. It provides a sublime method of encrypting information such the encrypted information such the attribute set that the descriptor must possess so as to decrypt the cipher-text. This is helpful for applications wherever the information provider knows specifically that user he needs to share with, in several applications the supplier can wish to share information according to some policy supported the receiving user's credentials.

III. PROPOSED WORK

Cipher text-Policy Attribute-based Encryption (CP-ABE) is considered one amongst the foremost appropriate technologies for information access management in cloud storage, as a result of this it provides data house owners a lot of direct management on access policies. Efficient method of classification by using cryptographic algorithm with the aim of achieving the required level of security. For encryption we are using bio-chaotic stream cipher that encrypts the iris images via the electronic media as well as it is used to encrypt the images in order to store into the databases for making them more secure with the help of biometric key and a bio-chaotic function.

IV. ARCHITCTURE & METHODOLOGY



As shown in fig 1, the data owner establishes the general public system parameter via Setup and generates a public/master-secret3 key try via Key info. Messages is encrypted via write by anyone World Health Organization additionally decides what cipher text category is related to the plaintext message to be encrypted. the info owner will use the master-secret to get AN combination cryptography key for a group of cipher text categories via Extract. The generated keys is passed to delegates firmly (via secure e-mails or secure devices) Finally, AN user with an combination key will decipher any cipher text only if the cipher text's category is contained within the combination key via decipher.

Key Generation: dead by the info owner to indiscriminately generate a public/master-secret key try.
Encrypt: dead by anyone World Health Organization desires to write information. On input a public-key pk, AN index I denoting the cipher text category, and a message m, it outputs a cipher text C.
Extracts: dead by the info owner for authorization the decrypting power for a particular set of cipher text categories to a delegate. On input the master-secret key msk and a group S of indice corresponding to completely different categories, it outputs the combination key for set S denoted by Kansas.
Decrypt: dead by a delegate World Health Organization received AN combination key Kansas generated by Extract. On input Kansas, the set S, AN index i denoting the cipher text category the cipher text C belongs to, and C, it outputs the decrypted result m if i two S.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106230 |

Methodology:

Mathematical Module
Let S ={SP, KG, En, Ex, Dn}

Where,

SP	setup an account on an untrusted server
KG	Key generation i.e Public /Master Key
En	Encrypt Data
Ex	Extract Aggregate key
Dn	Decrypt Data

Process:

1. Setup ($1^{\lambda}, n$) : Executed by the data owner to setup an account on an un trusted server
   Let g $\mathcal{E}\ G$ and $\alpha\ \epsilon_R \mathbb{Z}_p$
   Where G bilinear group and p is prime order
   Where $2^{\lambda} \leq p \leq 2^{\lambda+1}$
   Compute $g_i = g^{\alpha^i} \epsilon$ G
   Where i=1… n, n+2
   System parameter =(g, g1, ……., gn, gn+2)
2. Key Gen() : Executed by the data owner to randomly generate a public/master-secret key pair
   Select $\gamma\ \epsilon_R \mathbb{Z}_p$
   Where $\mathbb{Z}_p$ is prime number
   Out put the public and private key

3. Encrypt(pk, i, m) :Executed by anyone who wants to encrypt data.
   Let m be the message and be the index i
   Where m ϵG_T and i ϵ {1,2,….n}
   Let randomly select $t \in_R \mathbb{Z}_p$
   Where $\mathbb{Z}_p$ is prime number
   And compute the cipher text c as (g^t ,$(vg_i)^t$, m, $e(g1, gn)^t$)

4. Extract(msk = γ, s): Executed by the data owner for delegating the decrypting power For the set s of indices j's aggregate key is
   Ks = $\pi_{j \epsilon S} g^{\gamma}_{n+1-j}$
   Where S does not include 9, $g_{n+1-j} = g^{\alpha^{n_1-j}}$ always retrieve from param

5. Decrypt: (Ks, S, I, C) :Executed by a delegate who received an aggregate key KS generated by Extract
   Check if $i \notin S$ the out put $\perp$.
   Otherwise,
   Return message m= c3.e(Ks. $\pi_{j \epsilon S, j \neq i} g^{,c1}_{n+1-j+i}$,c1) /e($\pi_{j \epsilon S} g_{n+1-j}, c2$))

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106230 |

Let γ *be the knowlede of data owner* , the term $e(g1, gn)^t$ can be recoverd by e. $(c1, gn)^\gamma$ =e $(g^t, gn)^\gamma$ = e(g1', $gn)^t$

1. leakage-resilient cryptosystem:

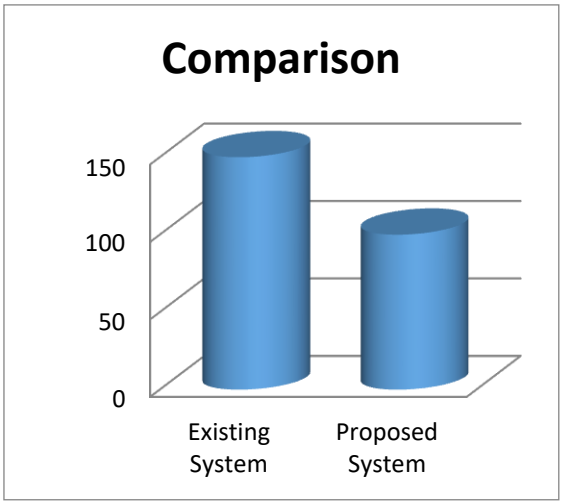
Public key Encryption scheme:
Let AE = (K, E, D) of PPT algorithm
Where k is input security parameter 1^λ ,
It outputs the public private key pair (pk, sk).

Where E gets as its input pk and message m ε M (M ,for some message space)
Its output is a cipher text c.

For decryption D on input the secrete key sk and α ciphertext c, the output a message m or $\perp$
Where the probability is taken over randomness of K, E, and D

V. EXPERIMENTAL RESULTS

Data Security in Cloud Using Key Aggregate Cryptosystem using the developed technique generates much less load on system about secret key as cyphertext classes increases. In order to show the effectiveness of the developed method over the conventional and state-of-the-art Key Aggregate Cryptosystem techniques, several example of different area with different features are used. We have checked our system on several input documents which are belongs to different category like Cryptographic Keys for a Predefined Hierarchy, Attribute-based encryption, Cloud Encryption Models, Compact Key in Identity-Based Encryption, Compact Key in Symmetric Key Encryption, etc. And every time our developed system has proved superiority among all existing systems



VII. CONCLUSION

In cloud storage users data privacy is a cardinal question . We consider how to compress secret keys in public-key cryptosystems which support delegation of secret keys for different cipher text classes in cloud storage. No matter which one among the power set of classes, the delegate can always get an aggregate key of constant size. In cloud storage, the number of cipher texts usually grows rapidly without any restrictions. So we have to reserve enough cipher text classes for the future extension. Otherwise, we need to expand the public-key. Although the parameter can be

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106230 |

downloaded with cipher texts, it would be better if its size is independent of the maximum number of cipher text classes.

The aggregate key encryption combined with ciphertext, which obviate attacks with high security. Key distribution can be managed easily with perfect security. The access policy and cryptographic schemes are getting more versatile and often involve multiple keys for a single application. Approach is more flexible than other key assignment which can only save a data.

REFERENCES

[1] Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, Senior Member," Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems. Volume: 25, Issue: 2. Year :2014.

[2] S.S.M. Chow, Y.J. He, L.C.K. Hui, and S.-M.Yiu, "SPICE – Simple Privacy-Preserving Identity-Management for Cloud Environment, "Proc. 10th Int'l Conf. Applied Cryptography and Network Security (ACNS), vol. 7341, pp. 526-543, 2012.

[3] B. Wang, S.S.M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," Proc. IEEE 33rd Int'l Conf. Distributed Computing Systems (ICDCS), 2013.

[4] S.S.M. Chow, C.-K.Chu, X. Huang, J. Zhou, and R.H. Deng, "Dynamic Secure Cloud Storage with Provenance," Cryptography and Security, pp. 442-464, Springer, 2012.

[5] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '03), pp. 416-432, 2003.

[6] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114, 2009.

[7] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans.Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.

[8] L. Hardesty, Secure Computers Aren't so Secure. MIT press, http://www.physorg.com/news176107396.html, 2009.

[9] G.Jai Arul Jose, C.Sajeev, "Implementation of Data Security in Cloud Computing",International Journals of P2P Network Trends and Technology, Vol. 1, Issue 1, 2011

[10] Yong Cheng, Jiangchun Ren, Zhiying Wang, "Attributes Union in CP-ABE Algorithm for Large Universe Cryptographic Access Control," Second International Conference on Cloud and Green Computing,pp.180-186, Nov 2012.

[11] Fengli Zhang, Qinyi Li, Hu Xiong, "Efficient Revocable Key-Policy Attribute Based Encryption with Full Security," Eighth International Conference on Computational Intelligence and Security,pp. 477-481,Nov 2012.

[12] W. Li, K. Xue, Y. Xue, and J. Hong, "TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 5, pp. 1484–1496, 2016.

[13] K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, "Combiningdata owner-side and cloud-side access control forencrypted cloud storage," IEEE Transactions on InformationForensics and Security, vol. 13, no. 8, pp. 2062–2074, 2018.

[14] A. Shamir, "How to share a secret," Communications ofthe ACM, vol. 22, no. 11, pp. 612–613, 1979.

[15] B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013.

[16] S. G. Akl and P. D. Taylor, "Cryptographic Solution to a Problem of Access Control in a Hierarchy," ACM Transactions on Computer Systems (TOCS), vol. 1, no. 3, pp. 239–248, 1983.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

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

Scan to save the contact details