International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-5, Issue-7 E-ISSN: 2347-2693

Secured Cloud Storage via Attribute-based Encryption

B. Sowmya[1*], K. Madhavi[2]

[1]Dept. of CSE, Gokaraju Rangaraju Institute of Engineering and Technology, Ranga Reddy, India
[2]Dept. of CSE, Gokaraju Rangaraju Institute of Engineering and Technology, Ranga Reddy, India

*Corresponding Author: sowmyabagari5@gmail.com

Available online at: www.ijcseonline.org

Received: 09/Jun/2017, Revised: 17/Jun/2017, Accepted: 15/Jul/2017, Published: 30/Jul/2017

Abstract— Cloud storage services have become increasingly popular. Because of the importance of privacy, many cloud storage encryption schemes have been struggle to protect data from the attackers. All of that schemes assumed that cloud storage providers are safe and it won't be target by the attackers; however, in practice, some government (i.e., coercers) may force cloud storage providers to expose user secrets or private data on the cloud, thus altogether avoid storage encryption schemes. In this paper, we present our design for a new cloud storage encryption scheme that enables cloud storage providers to create authentic fake user secrets to protect user privacy. By utilizing our systems scrambled information can be up to confidential regardless of the possibility that the capacity server is endowed; in addition, our techniques are secure against agreement assaults. Since coercers can't reveal if got privileged insights are valid or not, the distributed storage suppliers guarantee that client protection is still safely ensured. And we are also providing secret key mechanism which is aspired by KDC (Key distribution Center) one of the module and also authentication for each user to make the more secured and confidential. Were also captured the unauthorized attackers' information also.

Index Terms – Encryption, Attribute Based Encryption, Cloud Storage

I. INTRODUCTION

Cloud storage services have rapidly become increasingly popular. Users can store their data on the cloud and access their data anywhere at any time. Because of user privacy, the data stored on the cloud is typically encrypted and protected from access by other users. Considering the collaborative property of the cloud data, attribute-based encryption (ABE) is regarded as one of the most suitable encryption schemes for cloud storage. There are numerous ABE schemes that have been proposed [1,2,3,4,5,6,7,8,9,10].

Most of the proposed schemes assume cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked; however, in practice, some entities may intercept communications between users and cloud storage providers and then compel storage providers to release user secrets by using Government power or other means. For this situation, scrambled information is thought to be known and capacity suppliers are asked for to discharge client privileged insights. For instance, in 2010, without informing its clients, Google discharged client archives to the FBI subsequent to getting a court order [8]. In 2013, Edward Snowden uncovered the presence of worldwide recon-naissance programs that gather such cloud information as messages, messages, and voice messages from some innovation organizations [9,11,12]. When distributed storage suppliers are bargained, all encryption plans lose their viability. Despite the fact that we trust distributed storage suppliers can battle against such substances to keep up client security through lawful roads, it is seemingly more troublesome. As one illustration, Lavabit was an email benefit organization that shielded all client messages from outside pressure; shockingly, it fizzled and chosen to close down its email benefit. Since it is hard to battle against outside pressure, we intended to assemble an encryption plot that could help distributed storage suppliers stay away from this pickle. In our approach, we offer cloud storage providers means to create fake user secrets. Given such fake user secrets, outside coercers can only obtained forged data from a user's stored ciphertext. Once coercers think the received secrets are real, they will be satisfied and more importantly cloud storage providers will not have revealed any real secrets. Therefore, user privacy is still protected. This concept comes from a special kind of encryption scheme called *deniable encryption.* Deniable encryption involves senders and receivers creating convincing fake evidence of forged data in ciphertexts such that outside coercers are satisfied. Note that deniability comes from the fact that coercers cannot prove the proposed evidence is wrong and therefore have no reason to reject the given evidence. This approach tries to altogether block coercion efforts since coercers know that

their efforts will be useless. We make use of this idea such that cloud storage providers can provide audit-free storage services. In the cloud storage scenario, data owners who store their data on the cloud are just like senders in the deniable encryption scheme. Those who can access the encrypted data play the role of receiver in the deniable encryption scheme, including the cloud storage providers themselves, who have system wide secrets and must be able to decrypt all encrypted data1. In this work, we describe a deniable ABE scheme for cloud storage services. We make use of ABE characteristics for securing stored data with a fine-grained access control mechanism and deniable encryption to prevent outside auditing. Our plan depends on Waters ciphertext approach property based encryption (CP-ABE) scheme [4]. We upgrade the Waters conspire from prime request bilinear gatherings to composite request bilinear gatherings. By the subgroup choice issue suspicion, our plan empowers clients to have the capacity to give fake insider facts that appear to be genuine to outside coercers.

II. RELATED WORK ON ABE

The concept of ABE (Attribute-Based Encryption) in which data owners can insert how they want to distribute data in terms of encryption. That is, just the individuals who coordinate the proprietor's conditions can effectively decode put away information. We can state here that ABE is encryption for benefits, not for clients. This makes ABE an exceptionally supportive apparatus for distributed storage administrations since information sharing is a noteworthy component for such administrations. Distributed storage clients are not commonsense for information proprietors to encode their information by match astute keys. Moreover, it is additionally unreasonable to scramble information ordinarily for some individuals. With ABE, information proprietors settle on a choice just which sort of clients can get to their scrambled information. Clients who persuade the conditions can decode the encoded information.

Fuzzy IBE plan can be connected to empower encryption utilizing biometric contributions as characters; the mistake resilience property of a Fuzzy IBE conspire is definitely what takes into account the utilization of biometric personalities [2], which inalienably will have some clamor each time they are inspected. Also, we demonstrate that Fuzzy-IBE can be utilized for a kind of use that we term "quality based encryption". The Water and Sahai again dealt with ABE in another paper[3][4]; In this paper we display a framework for acknowledging complex get to control on scrambled information that we call Ciphertext-Policy Attribute-Based Encryption. By utilizing our strategies scrambled information can be kept confidential regardless of the possibility that the capacity server is entrusted; also, our techniques are secure against conspiracy assaults [2].

There are two sorts of ABE, CP-ABE and Key-Policy ABE (KP-ABE). The contrast between these two lies in strategy checking. KP-ABE is an ABE in which the arrangement is implanted in the client mystery key and the quality set is installed in the figure content. On the other hand, CP-ABE inserts the arrangement into the figure content and the client mystery has the characteristic set. Goyal et al. proposed the main KP-ABE [4].

Fuzzy Identity-Based Encryption

Author: *Amit Sahai, Brent Waters* We introduce a new type of Identity-Based Encryption (IBE) scheme that we call [2] Fuzzy Identity-Based Encryption. In Fuzzy IBE we view an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a ciphertext encrypted with an identity, ω0, if and only if the identities ω and ω0 are close to each other as measured by the "set overlap" distance metric. A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Additionally, we show that Fuzzy-IBE can be used for a type of application that we term "attribute-based encryption". In this paper we present two constructions of Fuzzy IBE schemes [2]. Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. We prove the security of our schemes under the Selective-ID security model.

Cipher text-Policy Attribute Base Decryption

Authors*: John Bethencourt, Amit Sahai, Brent Waters* In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. This paper presenting a system for realizing complex access control on encrypted data that call Ciphertext-Policy Attribute-Based Encryption [2]. By using this technique encrypted data can be kept confidential even if the storage server is entrusted; moreover, these methods are secure against collusion attacks. Previous Attribute-Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in this system attributes are used to describe a user's credentials and a party encrypting data determines a policy for who can decrypt. Thus, this method is conceptually closer to traditional access control methods such as RoleBased Access Control (RBAC).

In addition, it provides an implementation of our system and gives performance measurements.

Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data

Author: *Vipul Goyal Omkant Pandey Amit Sahai, Brent Waters* As more sensitive data is shared and stored by third-party site on the internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertext auserisable to decrypt. We demonstrate the applicability of our construction to sharing of auditlog information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

Deniable (CP-ABE): Our plan-ahead, bideniable and multidistributional CP-ABE scheme is composed of the following algorithms:

- Setup(1) → (PP,MSK): This algorithm takes security parameter as input and returns public parameter PP and system master key MSK.
- KeyGen(MSK, S) → SK: Given set of attributes S and MSK, this algorithm outputs private key SK.
- Enc(PP,M,A)→C:This encryption algorithm takes as input public parameter PP, message M, and LSSS access structure A = (M,) over the universe of attributes. This algorithm encrypts M and outputs a ciphertext C, which can be decrypted by those who possess an attribute set that, satisfies access structure A. Note that A is contained in C.
- Dec(PP, SK,C) → {M,⊥}: This decryption algorithm takes as input public parameter PP, private key SK with its attribute set S, and ciphertext C with its access structure A. If S satisfies A, then this algorithm returns M; otherwise, this algorithm returns ⊥.
- OpenEnc(PP,C,M) → PE: This algorithm is for the sender to release encryption proof PE for (M,C).OpenDec(PP, SK,C,M) → PD: This algorithm is for the receiver to release decryption proof PD for (M,C).
- Verify(PP,C,M, PE, PD) → {T, F}: This algorithm is used to verify the correctness of PE and PD

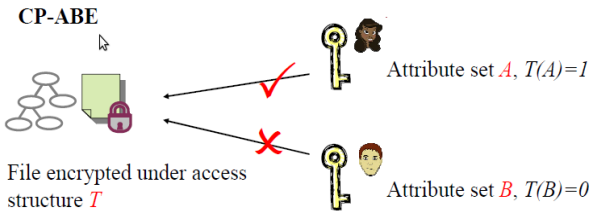

Fig.1: Ciphertext-Policy Attribute Based Encryption.

There are many scrambled component in market to secure the information however some of them are not legitimately actualized. A large portion of the proposed plans expect distributed storage specialist coops or trusted outsiders taking care of key administration are trusted and can't be hacked; For this situation, scrambled information are thought to be known and capacity suppliers are asked for to discharge client privileged insights.

It is additionally unreasonable to scramble information ordinarily for some individuals. With ABE, information proprietors choose just which sort of clients can get to their encoded information. Clients who fulfill the conditions can unscramble the scrambled information. Utilize translucent sets or simulatable open key frameworks to execute deniability. Most deniable open key plans are bitwise, which implies these plans can just process one piece a period; along these lines, bitwise deniable encryption plans are wasteful for genuine utilize, particularly in the distributed storage benefit case.

III. PROPOSED SYSTEM

In this work, we describe a deniable ABE scheme for cloud storage services. We make use of ABE characteristics for securing stored data with a fine-grained access control mechanism and deniable encryption to prevent outside auditing. We are also adding private key mechanism which is given by KDC and authentication for each user to make more secured about cloud storage. We are also maintains unauthorized attacker information. Our scheme is based on Waters ciphertext policy-attribute based encryption (CP-ABE) scheme. We improve the Waters conspire from prime request bilinear gatherings to composite request bilinear gatherings. By the subgroup choice issue supposition, our plan empowers clients to have the capacity to give fake insider facts that appear to be genuine to outside coercers. In this work, developing a deniable CP-ABE plot that can make distributed storage administrations secure and review free. In this situation, distributed storage specialist organizations are recently viewed as recipients in other deniable plans. Dissimilar to most past deniable encryption plans, it is not using translucent sets table open key frameworks to execute deniability. Rather, this embrace the thought proposed with a few upgrades. This develop deniable encryption plot through

a multidimensional space. All information is scrambled into the multidimensional space.

Not at all like most past deniable encryption plans, we don't utilize translucent sets or simulatable open key frameworks to execute deniability. Rather, we receive the thought proposed with a few changes. We develop our deniable encryption conspire through a multidimensional space. All information is encoded into the multidimensional space. In this work, we fabricate a predictable situation for our deniable encryption plot. By predictable condition, we imply that one encryption condition can be utilized for numerous encryption times without framework refreshes. It is more secured by private key instrument.

IV. SYSTEM ARCHITECTURE

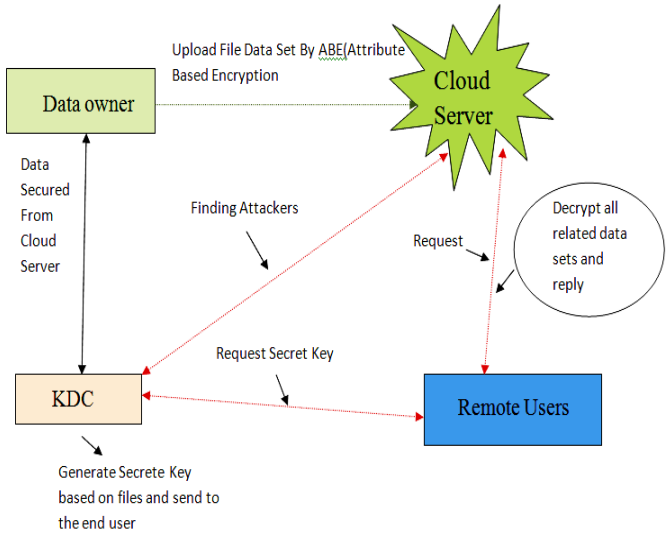

Fig.2: System Architecture

A. Data Owner

In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud. The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file.

B. Cloud Server

The cloud specialist organization deals with a cloud to give information stockpiling administration. Information proprietors encode their information documents and store them in the cloud for offering to information purchasers. To get to the common information records, information shoppers download encoded information documents of their enthusiasm from the cloud and after that decode them. It is responsible for authorizing all end users.

C. Key Distribution centre

KDC who is trusted to store confirmation parameters and offer open question administrations for these parameters, for example, creating mystery key in light of the document and send to the comparing end clients. It is responsible for capturing the attackers.

D. Data Consumer/End User

In this module, the client can just get to the information document with the encoded key if the client has the benefit to get to the record. For the client level, every one of the benefits are given by the Data proprietor and the Data clients are controlled by the information proprietor as it were. Clients may attempt to get to information records either inside their get to benefits, so pernicious clients may plot with each other to get delicate documents past their benefits. He is sending solicitation to KDC to produce mystery key and KDC will create the key and send to comparing end client.

E. Attacker (Unauthorized User)

Attackers add the malignant information to a piece in cloud server. At that point the unauthorized client will considered as an attackers.`

V. CONCLUSIONS

In this work, we proposed a deniable CP-ABE plan to construct a review free distributed storage benefit. The deniability highlight makes pressure invalid, and the ABE property guarantees secure cloud information imparting to a fine-grained get to control component. Our proposed conspire gives a conceivable approach to battle against indecent obstruction with the privilege of security. We trust more plans can be made to ensure cloud client protection.

REFERENCES

[1] Shreeraghav kulkarni, Sujata Terdal, "*Ttpse- Trusted Third Party With Symmetric Encryption Towards Secured Cloud Storage*", International Journal of Computer Sciences and Engineering, Vol.5, Issue.5, pp.47-51, 2017.

[2] V. Kapoor, "*Data Encryption and Decryption Using Modified RSA Cryptography Based on Multiple Public Keys and 'n'prime Number*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.2, pp.35-38, 2013.

[3] A. Sharma, RS Thakur, S. Jaloree, "*Investigation of Efficient Cryptic Algorithm for image files Encryption in Cloud*", International Journal of Scientific Research in Computer Science and Engineering, Vol.4, Issue.5, pp.5-11, 2016.

[4] S. Mewada, P. Sharma, and S. S. Gautam, "*Investigation of Efficient Cryptic Algorithm for Text using SM Crypter*", International Journal of Information Science and Computing, vol. 3, no. 2, p. 99, 2016.

[5] A. Sahai, H. Seyalioglu, and B. Waters, "*Dynamic credentials and ciphertext delegation for attribute-based encryption*", in Crypto, 2012, pp. 199–217.

[6] S. Hohenberger and B. Waters, "*Attribute-based encryption with fast decryption*", in Public Key Cryptography, 2013, pp. 162–179.

[7] P. K. Tysowski and M. A. Hasan, "*Hybrid attribute and reencryption based key manage-ment for secure and scalable*

mobile app-lications in clouds", IEEE T. Cloud Computing, pp. 172–186, 2013.

[8] D. Bradbury, "*Can we make email secure?",* Network Security, vol. 2014, no. 3, pp. 13–16, Mar. 2014.

[9] P.-W. Chi and C.-L. Lei, "*Audit-Free Cloud Storage via Deniable Attribute-based Encryption*", IEEE Transactions on Cloud Computing, pp. 1–1, 2015.

[10] R. F. Anda, A. Butchart, V. J. Felitti, and D. W. Brown, "*Building a Framework for Global Surveillance of the Public Health Implications of Adverse Childhood Experiences*", American Journal of Preventive Medicine, vol. 39, no. 1, pp. 93–98, Jul. 2010.

[11] Surbhi Sharma, "*Embedding more security in digital signature system by using combination of public key cryptography and secret sharing scheme*", International Journal of Computer Sciences and Engineering, Vol.4, Issue.3, pp.111-115, 2016.

[12] P.Gasti, G.Ateniese, and M. Blanton, "*Deniable cloud storage: sharing files via public-key deniability*", Proceedings of the 9th annual ACM workshop on Privacy in the electronic society, pp. 31– 42, 2010.

