International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 5, 2016. ISSN: 2348-6600
Reference ID: IJCS-139 PAGE NO: 820-826

KP-ABE Security & Encryption on Cloud Data Storage System

M AMARESWARA KUMAR[1]&HUSSAIN BASHA SHAIK[2]

[1]ASSISTANT PROFESSOR Dept. of CSE SVR ENGINEERING COLLEGE, AYYALURU, NANDYAL Email: -a.amar1202@gmail.com

[2]PG-Scholar Dept. of CSE SVR ENGINEERING COLLEGE, AYYALURU, NANDYAL Email: - hussainbashandl.basha@gmail.com

***Abstract*—** Cloud storage accommodations have become increasingly popular. Because of the paramountcy of privacy, many cloud storage encryption schemes have been proposed to forfend data from those who do not have access. All such schemes surmised that cloud storage providers are safe and cannot be hacked; however, in practice, some ascendant entities (i.e., coercers) may force cloud storage providers to reveal utilizer secrets or confidential data on the cloud, thus altogether circumventing storage encryption schemes. In this paper, we present our design for an incipient cloud storage encryption scheme that enables cloud storage providers to engender convincing fake utilizer secrets to forfend utilizer privacy. Since coercers cannot tell if obtained secrets are true or not, the cloud storage providers ascertain that utilizer privacy is still securely forfended.

Keywords: - Controvertible Encryption, attribute encryption scheme, cloud storage, bilinear order.

1. INTRODUCTION

Attribute Based Encryption is proposed by sahai and is able to effectively increase the exibility of data sharing such that only parties satisfying special policy are allowed to access the data. It comes in two flavors: one is the key policy ABE (KP ABE), and the other is the cipher text policy ABE (CP - ABE). In the former, cipher text are labelled with attribute sets and private keys are associate with entrance structure that allude which class of cipher text that receiver is able to decrypt. However, the case is complementary. That is, cipher text are relevant to access structures, and ascribe sets are associate to private keys. Attribute based encryption is applicable to many network applications, such as targeted broadcast and multi-cost. Consider the collaborative attribute of the cloud information, attribute based encryption (ABE) is regarded as one of the most compatible encryption schemes for cloud storage. There are

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 5, 2016. ISSN: 2348-6600
Reference ID: IJCS-139 PAGE NO: 820-826

numerous schemes, that have been propose Most of the proposed schemes are used by the cloud storage service providers or believe third parties handling key management are trusted and cannot be hack; Sometimes may intermediate communications between users and cloud storage providers and then compel storage providers to deliver user secrets by using government power or other means. In this case, encrypted information and storage providers are requested to reveal the user secrets. The FBI after their effectiveness. Though we trust cloud storage providers can fight versus such entities to maintain user privacy through jural avenues, it is seemingly considerable and more difficult. As one instance, Lava bit was an electronic mail service company that protect all user emails from outside coercion; unfortunately, it shut down for email service at error occur. Offence it is arduous to fight against outside coercion, we aimed to context an encryption scheme that could help cloud storage providers. In our contribution, we offer the cloud storage providers means to fabricate fake user secrets. Given such fake user confidential data is outside coercers can only obtained forged information from a user's stored cipher text.once the coercers think the received secrets are true, they will be satisfy and mightly importantly cloud supply providers will not have released any true secrets. Therefore, the user privacy is still protected in cloud.

2. RELATED WORK

Subsisting system

There are numerous ABE schemes that have been proposed. Most of the proposed schemes surmise cloud storage accommodation 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 relinquish utilizer secrets by utilizing regime power or other betokens. In this case, encrypted data are postulated to be kenned and storage providers are requested to relinquish utilizer secrets. Sahai and Waters first introduced the concept of ABE in which data owners can embed how they optate to apportion data in terms of encryption. There are two types of ABE, CP-ABE and Key-Policy ABE (KP-ABE). Goyal et al. proposed the first KPABE. They constructed an expressive way to relate any monotonic formula as the policy for utilizer secret keys. Bettencourt et al. proposed the first CP-ABE. This scheme utilized a tree access structure to express any monotonic formula over attributes as the policy in the cipher

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 5, 2016. ISSN: 2348-6600
Reference ID: IJCS-139 PAGE NO: 820-826

text. It is withal impractical to encrypt data many times for many people. With ABE, data owners decide only which kind of users can access their encrypted data. Users who satiate the conditions are able to decrypt the encrypted data. Utilize translucent sets or simulatable public key systems to implement deniability. Most disputable public key schemes are bitwise, which denotes these schemes can only process one bit a time; consequently, bitwise disputable encryption schemes are inefficient for authentic use, especially in the cloud storage accommodation case. Most of the anterior disputable encryption schemes are inter-encryption independent. That is, the encryption parameters should be consummately different for each encryption operation. If two controvertible encryptions are performed in the same environment, the latter encryption will lose deniability after the first encryption is coerced, because each coercion will reduce flexibility. Most controvertible encryption schemes have decryption error quandaries. These errors emanate from the designed decryption mechanisms.

Proposed system

In this work, we describe a controvertible ABE scheme for cloud storage accommodations. We make utilization of ABE characteristics for securing stored data with a fine-grained access control mechanism and controvertible encryption to avert outside auditing. Our scheme is predicated on Waters cipher text policy-attribute predicated encryption (CP-ABE) scheme. We enhance the Waters scheme from prime order bilinear groups to Composite order bilinear groups. By the subgroup decision quandary postulation, our scheme enables users to be able to provide fake secrets that seem legitimate to outside coercers. In this work, we construct a controvertible CP-ABE scheme that can make cloud storage accommodations secure and audit free. In this scenario, cloud storage accommodation providers are just regarded as receivers in other disputable schemes. Unlike most anterior controvertible encryption schemes, we do not utilize translucent sets or simulatable public key systems to implement deniability. Instead, we adopt the conception proposed with some ameliorations. We construct our disputable encryption scheme through a multidimensional space. All data are encrypted into the multidimensional space. Only with the correct composition of dimensions is the pristine data obtainable. With mendacious composition, ciphertexts will be decrypted to predetermined fake data. The information defining the dimensions is

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 5, 2016. ISSN: 2348-6600
Reference ID: IJCS-139 PAGE NO: 820-826

kept secret. We make utilization of composite order bilinear groups to construct the multidimensional space. We withal use chameleon hash functions to make both true and fake messages convincing. In this work, we build a consistent environment for our controvertible encryption scheme. By consistent environment, we designates that one encryption environment can be utilized for multiple encryption times without system updates. The opened receiver proof should look cogent for all ciphertexts under this environment, regardless of whether a cipher text is customarily encrypted or disputably encrypted. The deniability of our scheme emanates from the secret of the subgroup assignment, which is tenacious only once in the system setup phase. By the abrogating property and the opportune subgroup assignment, we can construct the relinquished fake key to decrypt mundane ciphertexts correctly.

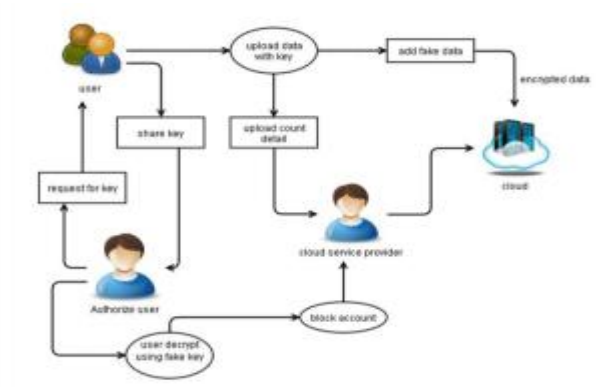

Fig:-1 System architecture

3. IMPLEMENTATION

Data Owner

The data owners resort to the TPA for integrity verification and delegate the reparation to the proxy. In the file upload module mainly fixate on the upload file in the cloud. The file is uploading by utilizer in the cloud with the encryption key. Withal insert the fictitiously unauthentic file to the pristine file. The sanction utilizers download the file utilizing the decryption key. The file store in the cloud after the encryption process. There is more of utilizer store the information in the cloud because storing in cloud the security. The utilizer stores the pristine data in cloud. The data may be hack by sanction utilizer.

Cloud

Which are managed by the cloud accommodation provider, provide storage accommodation and have paramount computational resources. In this work, we construct a controvertible CP-AB ENCRYPTION scheme that can make cloud storage accommodations secure and audit free. In this scenario, cloud storage accommodation providers are just regarded as receivers in other controvertible schemes. Unlike most antecedent controvertible.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 5, 2016. ISSN: 2348-6600
Reference ID: IJCS-139 PAGE NO: 820-826

Third Party Auditor

Who has expertise and capabilities to conduct public audits on the coded data in the cloud, the TPA is trusted and its audit result is equitable for both data owners and cloud servers. Deterministic Decryption. Most controvertible encryption schemes have decryption error quandaries. These errors emanate from the designed decryption mechanisms. For example, in, Canetti et al. utilizes the subset decision mechanism for decryption. The receiver determines the decrypted message according to the subset decision result. If the sender culls an element from the ecumenical set but infelicitously the element is located in the categorical subset, then an error occurs. The same error occurs in all translucent set predicated controvertible encryption schemes. Another example is in which utilizes a voting mechanism for decryption. Decryption is veridical if and only if the correct part inundates the mendacious part. Otherwise, the receiver will get the error result. The concept of our disputable scheme is different than these schemes described above. Our scheme elongates a pairing ABE, which has a deterministic decryption algorithm, from the prime order group to the Composite order group. The decryption algorithm in our scheme.

4. EXPERIMENTAL RESULTS

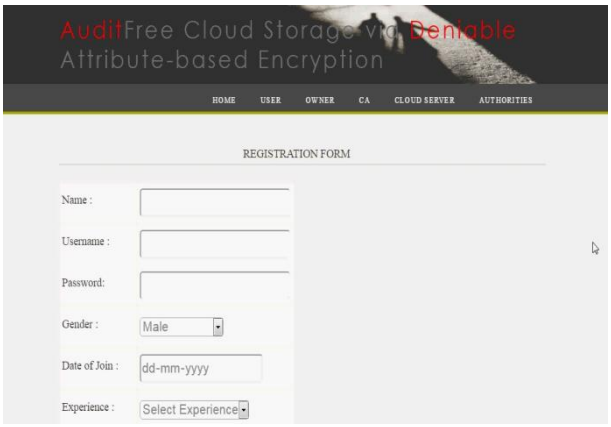

Fig:-2 New User Registration

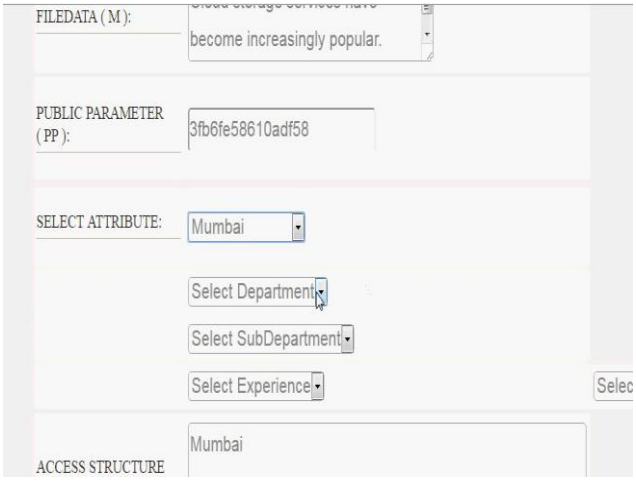

Fig:-3 ABE Structure

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 5, 2016. ISSN: 2348-6600
Reference ID: IJCS-139 PAGE NO: 820-826

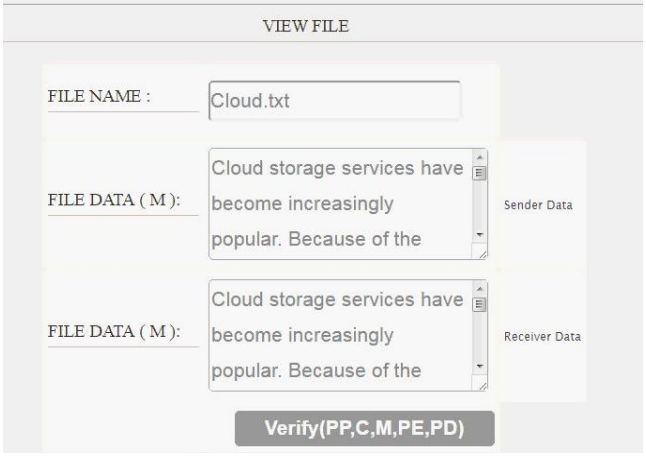

Fig:-4 File Data in Blocks & Verifying

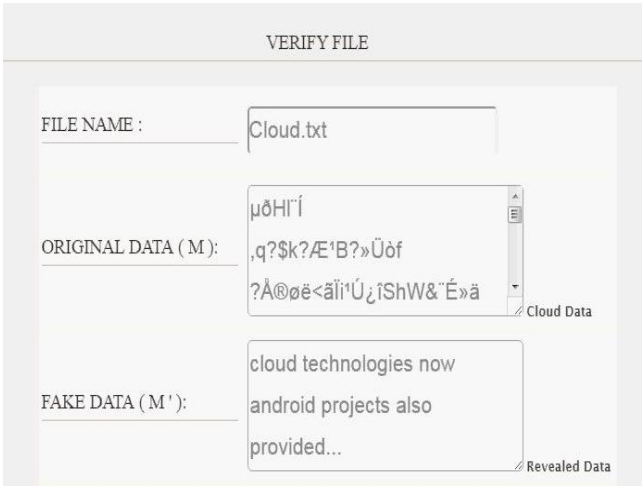

Fig:-5 Data Encryption.

5. CONCLUSION

In this paper, a disputable CP-ABE schemes to context an audit-free cloud storage accommodation. The deniability feature makes coercion powerless, and the ABE property ascertain the cloud information is securely sharing with a fine-grained International Journal of Engineering Science and Computing access control mechanism. Our view in this scheme provides a possible way to fight against immoral obstacles with the right of utilizer privacy. We trust the more encryption schemes can be proposed to bulwark the cloud utilizer privacy.

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Eurocrypt, 2005, pp. 457–473.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in ACM Conference on Computer and Communications Security, 2006, pp. 89–98.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in IEEE Symposium on Security and Privacy, 2007, pp. 321–334.

[4] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography, 2011, pp. 53–70.

[5] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 5, 2016. ISSN: 2348-6600
Reference ID: IJCS-139 PAGE NO: 820-826

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 management for secure and scalable mobile applications in clouds." IEEE T. Cloud Computing, pp. 172–186, 2013.

[8] Wired. (2014) Spam suspect uses google docs; fbi happy. [Online]. Available: http://www.wired.com/2010/04/cloud-warrant/

[9] Wikipedia. (2014) Global surveillance disclosures (2013present).[Online]. Available: http://en.wikipedia.org/wiki/Global surveillance disclosures (2013-present)

[10] (2014) Edward snowden. [Online]. Available: http://en. wikipedia.org/wiki/Edward Snowden.