

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

Attribute Based Encryption System in an Audit-Free Cloud Storage

K.Pranathi¹, M .Deena Babu² M.Tech (Ph.D)

P.G. Student Department of Computer Science & Engineering, Malla Reddy Institute of Technology, India¹

Associate Professor, Department of Computer Science & Engineering, Malla Reddy Institute of Technology, India²

ABSTRACT: Cloud storage services have become increasingly popular. Because of the importance of privacy, many cloud storage encryption schemes have been proposed to protect data from those who do not have access. All such schemes assumed that cloud storage providers are safe and cannot be hacked; however, in practice, some authorities (i.e., coercers) may force cloud storage providers to reveal user secrets or confidential data on the cloud, thus altogether circumventing storage encryption schemes. In this paper, we present our design for a new cloud storage encryption scheme that enables cloud storage providers to create convincing fake user secrets to protect user privacy. Since coercers cannot tell if obtained secrets are true or not, the cloud storage providers ensure that user privacy is still securely protected.

KEYWORDS: Cloud Storage, Encryption Schemes, Co-ercers, Cloud-storage Providers.

I. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers. 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. The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things. A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making..

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

II. LITERATURE SURVEY

a) Fuzzy Identity-Based Encryption: We introduce a new type of Identity-Based Encryption (IBE) scheme that we call 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, ω' , if and only if the identities ω and ω' 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”.

b) Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data: As more sensitive data is shared and stored by third-party sites 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, 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. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

c) Cipher text-Policy Attribute-Based Encryption: In several distributed systems a user should only be able to access data if a user possesses 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. In this paper we present a system for realizing complex access control on encrypted data that we call Cipher text-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our 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 our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

d) Cipher text-policy attribute-based encryption: An expressive, efficient, and provably secure realization: We present a new methodology for realizing Cipher text-Policy Attribute Encryption (CP-ABE) under concrete and no interactive cryptographic assumptions in the standard model. Our solutions allow any encryptor to specify access control in terms of any access formula over the attributes in the system. In our most efficient system, cipher text size, encryption, and decryption time scales linearly with the complexity of the access formula. The only previous work to achieve these parameters was limited to a proof in the generic group model. We present three constructions within our framework. Our first system is proven selectively secure under a assumption that we call the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption which can be viewed as a generalization of the BDHE assumption. Our next two constructions provide performance tradeoffs to achieve provable security respectively under the (weaker) decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman assumptions.

e) Dynamic credentials and ciphertext delegation for attribute-based encryption: Motivated by the question of access control in cloud storage, we consider the problem using Attribute-Based Encryption (ABE) in a setting where users' credentials may change and ciphertexts may be stored by a third party. Our main result is obtained by pairing two contributions: We then combine these two results for a new approach for revocation on stored data. Our scheme allows a storage server to update stored ciphertexts to disqualify revoked users from accessing data that was encrypted before the user's access was revoked while key update broadcasts can dynamically revoke selected users.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

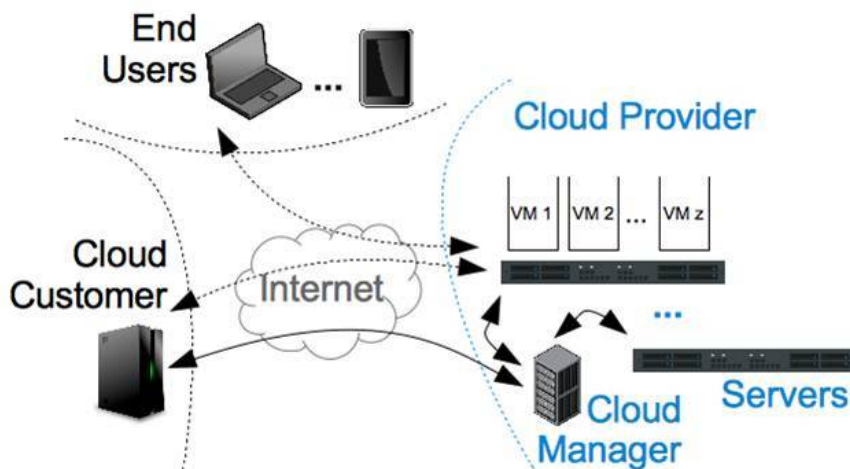
Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

III. PROPOSED METHODOLOGY AND DISCUSSION

There are numerous ABE schemes that have been proposed. 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. In this case, encrypted data are assumed to be known and storage providers are requested to release user secrets. Sahai and Waters first introduced the concept of ABE in which data owners can embed how they want to share data in terms of encryption. But .it is 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 satisfy the conditions are able to decrypt the encrypted data .Most deniable public key schemes are bitwise, which means these schemes can only process one bit at a time; therefore, bitwise deniable encryption schemes are inefficient for real use, especially in the cloud storage service case. 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 scheme is based on Waters cipher text policy-attribute based encryption (CP-ABE) scheme. We enhance the Waters scheme from prime order bilinear groups to composite order bilinear groups. By the subgroup decision problem assumption, our scheme enables users to be able to provide fake secrets that seem legitimate to outside coercers .In this work, we construct a deniable CP-ABE scheme that can make cloud storage services secure and audit free. In this scenario, cloud storage service providers are just regarded as receivers in other deniable schemes. Unlike most previous deniable encryption schemes, we do not use translucent sets or simulatable public key systems to implement deniability. Instead, we adopt the idea proposed with some improvements. We construct our deniable encryption scheme through a multidimensional space. All data are encrypted into the multidimensional space. Only with the correct composition of dimensions is the original data obtainable. With false composition, cipher texts will be decrypted to predetermined fake data. The information defining the dimensions is kept secret. We make use of Composite order bilinear groups to construct the multidimensional space. We also use chameleon hash functions to make both true and fake messages convincing.

IV. SCHEME DESCRIPTION



International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

a) Key Distribution Center

In this module, we develop the Key Distribution Center (KDC). KDC provides the accessibility of files to users. Initially User will request for a secret key pair for the selected file. The respective public and private key credentials will be sent to the Email ID of users by key distribution centre. To build an audit-free secure cloud storage service, we use a deniable CP-ABE scheme as our core technology.

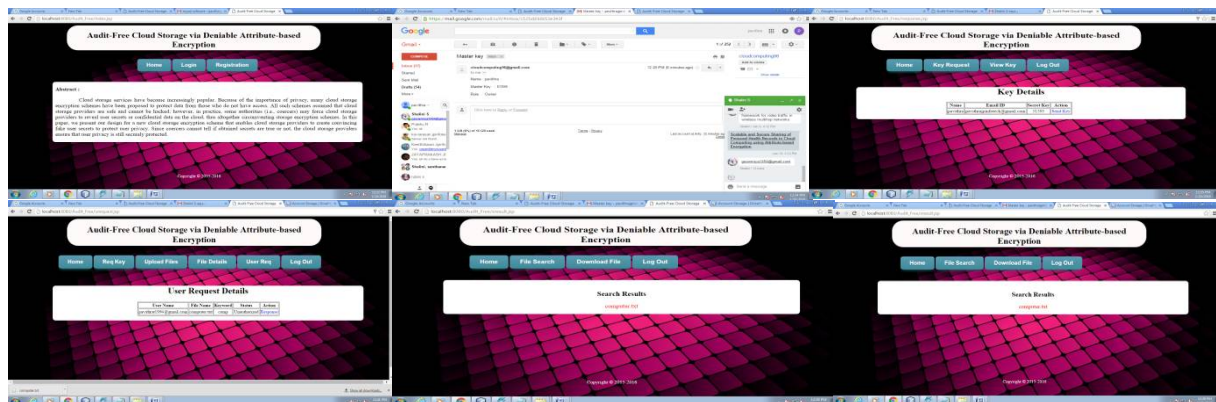
b) Data Owners: The proposed scheme should allow new data owners to enter this system without affecting other data owners or data users, i.e., the scheme should support data owner scalability in a plug-and-play model. To prove that our deniable encryption scheme is secure requires this scheme to be a valid encryption scheme. For a multi-distributional deniable encryption scheme, it is only necessary to prove the security from the normal algorithm set.

c) Cloud Server: Then, the owner sends the encrypted data to the cloud server. They do not rely on the server to do data access control. But, the access control happens inside the cryptography. That is only when the user's attributes satisfy the access policy defined in the cipher text; the user is able to decrypt the ciphertext. Thus, users with different attributes can decrypt different number of content keys and thus obtain different granularities of information from the same data.

d) User Module: Each user has a global identity in the system. A user may be entitled a set of attributes which may come from multiple attribute authorities. The user will receive a secret key associated with its attributes entitled by the corresponding Key Distribution Centre. A user can obtain the true message with a valid secret key, regardless of whether the ciphertext is normally encrypted or deniably encrypted.

e) Search over Files: The proposed scheme should allow search over encrypted files which would be encrypted and stored in the cloud. This functionality provides you the facility of searching respective file with a searching text. This will leads to ask for a secret key. Then the credentials will help to achieve file download

V. EXPERIMENTAL RESULTS



VI. CONCLUSION

In this work, we proposed a deniable CP-ABE scheme to build an audit-free cloud storage service. The deniability feature makes coercion invalid, and the ABE property ensures secure cloud data sharing with a fine-grained access control mechanism. Our proposed scheme provides a possible way to fight against immoral interference with the right of privacy. We hope more schemes can be created to protect cloud user privacy.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

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 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_\(2013-present\)](http://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013-present))
- [10] ———. (2014) Edward snowden. [Online]. Available: http://en.wikipedia.org/wiki/Edward_Snowden
- [11] ———. (2014) Lavabit. [Online]. Available: <http://en.wikipedia.org/wiki/Lavabit>
- [12] R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, "Deniable encryption," in *Crypto*, 1997, pp. 90–104.
- [13] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Eurocrypt*, 2010, pp. 62–91.
- [14] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. R'afols, "Attribute-based encryption schemes with constant-size ciphertexts," *Theor. Comput. Sci.*, vol. 422, pp. 15–38, 2012.
- [15] M. D'urumuth and D. M. Freeman, "Deniable encryption with negligible detection probability: An interactive construction," in *Eurocrypt*, 2011, pp. 610–626.
- [16] A. O'Neill, C. Peikert, and B. Waters, "Bi-deniable public-key encryption," in *Crypto*, 2011, pp. 525–542.
- [17] P. Gasti, G. Ateniese, and M. Blanton, "Deniable cloud storage: sharing files via public-key deniability," in *WPES*, 2010, pp. 31–42.
- [18] M. Klonowski, P. Kubiak, and M. Kutylowski, "Practical deniable encryption," in *SOFSEM*, 2008, pp. 599–609.
- [19] M. H. Ibrahim, "A method for obtaining deniable public-key encryption," *I. J. Network Security*, vol. 8, no. 1, pp. 1–9, 2009.
- [20] J. B. Nielsen, "Separating random oracle proofs from complexity theoretic proofs: The non-committing encryption case," in *Crypto*, 2002, pp. 111–126