International Journal of Research

Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 13
September 2016

Audit-Free Cloud Storage via Deniable Attribute-based Encryption

Mr.BASANI PRADEEP KUMAR

Mr. K.Raju

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.

Index Terms—Deniable Encryption, Composite Order Bilinear Group, Attribute-Based Encryption, Cloud Storage

1 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, including [1], [2], [3], [4], [5], [6], [7].

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. As an example, in 2010, without notifying its users, Google released user documents to the FBI after receiving a search warrant [8]. In 2013, Edward Snowden disclosed the existence of global surveillance programs that collect such cloud data as emails, texts, and voice messages from some technology companies [9], [10]. Once cloud storage providers are compromised, all encryption schemes lose their effectiveness. Though we hope cloud storage providers can fight against such entities to maintain user privacy through legal avenues, it is seemingly more and more difficult. As one example, Lavabit was an email service company that protected all user emails from outside coercion; unfortunately, it failed and decided to shut down its email service [11].

2 DEFINITION

2.1 Deniable CP-ABE Scheme

Deniable encryption schemes may have different properties and we provide an introduction to many of these properties below.

• *ad hoc deniability vs. plan-ahead deniability*: The former can generate a fake message (from the entire message space) when coerced, whereas the latter requires a predetermined fakemessage for encryption. Undoubtedly, all bitwise encryption schemes are ad hoc.

• *sender-, receiver-, and bi-deniability*: The prefix here in each case implies the role that can fool the coercer with convincing fake evidence. In sender-deniable encryption schemes and receiver-deniable schemes, it is assumed that the other entity cannot be coerced. Bi-deniability means both sender and receiver can generate fake evidence to pass third-party coercion.

• *full deniability vs. multi-distributional deniability*: A fully deniable encryption scheme is one in which there is only one set of algorithms, i.e., a keygeneration algorithm, an encryption algorithm and so on. Senders, receivers and coercers know this set of algorithms and a sender and a receiver can fool a coercer under this condition. As for multi distributional deniable encryption schemes, there are two sets of algorithms, one being a normal set, while the other is a deniable set. The outputs of algorithms in these two sets are computationally indistinguishable. The normal set of algorithms cannot be used to fool coercers, whereas the deniable set can be used. A sender and a receiver can use the deniable algorithm set, but claim that they use the normal algorithm set to fool coercers..

• *interactive encryption vs. non-interactive encryption*: The difference between these two types of encryption is that the latter scheme does not need interaction between sender and receiver.

According to the above definitions, the ideal deniable encryption scheme is *ad hoc*, *full*, *bi-deniability* and *non- interactive deniability*; however, there is research focused on determining the limitations of the deniable schemes. IN [20], Nielsen stated that it is impossible to encrypt unbounded messages by one short key in non-committing schemes, including deniable schemes. Since we want our scheme to be blockwise deniable with a consistent encryption environment, we design our scheme to be a plan-ahead deniable encryption scheme. In [21], Bendlin et al. showed that non-interactive and fully receiverdeniable properties cannot be achieved simultaneously. We prefer our scheme to have the non-interactive property for ease of use. Therefore, our scheme is multidistributional. In summary, our deniable scheme is planahead, bi-deniable, and multi-distributional. Below, we provide the definition of this kind of deniable CP-ABE scheme.

3.1.1 Is a Confidential PK Practical?

In the above definition, our scheme assumes that PK will be kept secret from the coercer. Some may argue that it is impractical, stating that coercers can pretend to be users in cloud storage services and obtain the PK. Once the PK is released to coercers, they can easily generate deniably encrypted ciphertexts and use these ciphertexts to determine the types of receiver proofs. To address this question, we must return to the basic assumption of deniable encryption schemes, i.e., **senders and receivers want to hide their communication messages from outside coercers**. Like all other cryptographic schemes, secrets must be assumed to be unknown to adversaries and our scheme is no exception. Therefore assuming that the PK is kept secret to coercers is acceptable and unavoidable.

To keep PK secret, cloud service providers can integrate deniable CP-ABE schemes with their own user authentication mechanisms. Note that in our definition, a deniable CP-ABE scheme can enable cloud storage service providers to offer two kinds of storage services, one being normal storage service, the other being auditfree storage service. So a user can choose to enjoy normal cloud storage services through a basic authentication process or enjoy audit-free cloud storage services through a much more sincere authentication process. Therefore, we believe our idea can be used to build practical cloud storage services, especially for those communities who currently have serious authentication processes.

one-time signature is used to maintain the integrity of the ciphertext. Using the same technique, we can enhance our CPA secure deniable CP-ABE scheme to be a CCA secure deniable CP-ABE scheme, as demonstrated in [31].

4 CONCLUSIONS

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.

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)

[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¨urmuth and D. M. Freeman, "Deniable encryption with negligible detection probability: An interactive construction," in *Eurocrypt*, 2011, pp. 610–626.

Author's Profile

Mr. K.Raju received M.Tech degree from Jayamukhi Institute of Technological Science,Narsampet, Warangal affiliated to JNTUH, Hydearabad. He is currently working as Assistant professor, Department of CSE, in Vinuthna Institute of Technology & Science ,Hasanparthy, Warangal, Telangana, India. Hisinterest includes Data Base Management Systems.

Mr.BASANI PRADEEPKUMAR recived B.Tech Degree from Vinuthna Institute of Technology and Science Hasanparty, Affliated to Kakatiya University (KU) Warangal.