International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 09 | Sept -2020 ISSN: 2582-3930

A New Encrypted Data Switching Protocol- Bridging IBE and ABE without Loss of Data Confidentiality

[1] Surya. S, [2]Ramya. K, [3]Bala Subramanian. N, [4]Mohamed Rafi. M

[1]Final year MCA, Mohamed Sathak Engineering College, Kilakarai

[3]Associate Professor, Dept of MCA, Mohamed Sathak Engineering College, Kilakarai

[4]Associate Professor, Dept of MCA, Mohamed Sathak Engineering College, Kilakarai

[2]Professor, HOD, Dept of MCA, Mohamed Sathak Engineering College, Kilakarai

ABSTRACT:

Cloud computing being a cutting-edge technology is one of the major technological revolutions in the century. It has led in a significant amount of data stored, computed and applied in big data. It has enormous advantage in applications of resource-limited, such as mobile devices, smart devices, and smart city and wireless body area networks. In Previous work, Homomorphic token encryption technology is used to encrypt and decrypt the file in cloud. Since it keeps same key for both client side and server side, data may be leaked and hacked by intruders.

In proposed system, IBE-ABE have been introduced in the literature to enhance fine-grained data sharing by allowing data encryptor to encrypt data under the fuzzy information of data receiver.

1. INTRODUCTION

This process considers the conversion between conventional identity-based and attribute-based encryptions and further proposes a concrete construction via the technique of proxy re-encryption. The construction is proved to be CPA secure in the standard model under q-decisional parallel bilinear Diffie-Hellman exponent assumption.

The performance comparisons highlight that our bridging mechanism reduces computation and communication cost on the client side, especially when the data of the client is encrypted and outsourced to a remote cloud. The computational costs with respect to re-encryption (on the server

side) and decryption (on the client side) are acceptable in practice. Designing an encryption switching scheme to bridge IBE and ABE via proxy re-encryption (PRE) technique.

The efficiency analysis has highlighted that our solution outperforms the download-and-re-encrypt conversion mode. We improve computation and communication cost.

Identity-based cryptography is a general extension of public-key cryptography where the public key of a user can be any arbitrary string uniquely representing the identity of the user. ABE allows private key and ciphertext to be labeled with descriptions, so that a decryption is valid if and only if the description of a decryption key matches that of a ciphertext. It has been widely employed in fine-grained data access control. The efficiency analysis has highlighted that our solution outperforms the download-and-re-encrypt conversion mode computation and communication cost.

2. PROBLEM DESCRIPTION

In Existing system a cloud model, there are multiple owners who may encrypt according to their own ways, possibly using different sets of cryptographic keys.

But there is no security key to enter into cloud services for both admin and users. So that someone hack and modify the data in cloud easily. It poses a serious risk on both clients' privacy and intellectual property of monitoring service providers. We could not deter the wide adoption of cloud technology.

3. PLANNED DESIGN

1. Cloud

In this module, even ever cloud will login to the site, they can view all data owner information, and end user information like, their name, address, mobile number,etc. Cloud only have the rights to reencrypt the file content from the server which are uploaded by the data owner. Finally cloud can view all download file details.

2. Data Owner

In this module, data owner can register in to the site and then they get username, password. According to the username & password they login to the site, they upload the files with encryption format to the server. they can view their own uploaded files from the server. If the user need the files from the server they request to corresponding file owner. Even ever data owner need to the download their files they must get IBE file key and ABE file key to decrypt the content before download the file.

3. User

In this module, if the user need the file from server. they first register into the site and then they get username, password. Based on the username and password they enter into the site. if the user need any files from the server they request to the data owner. they may search and download the file from the server.

4. File Details

In this module, file contents are encrypted by IBE and ABE algorithm under cloud control. This encryption process is done by file key generation. if the data owner as well as data user need the file means they get the file key and decrypt the file content and finally download the file.

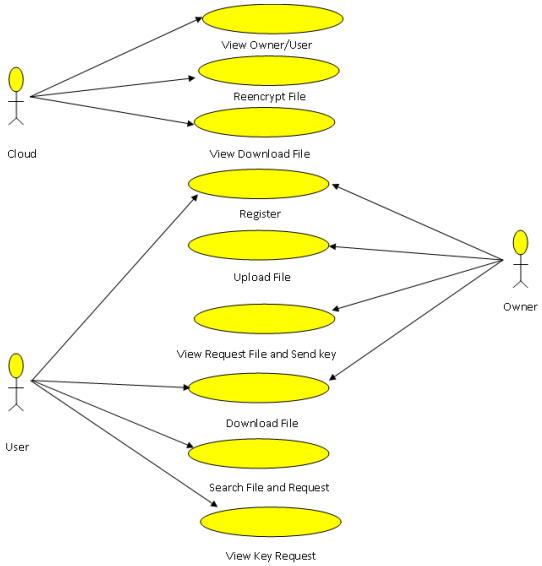
5. Request Details

In this module, if the user need any files from the server they request to the data owner. This request information is passed to the data owner. user will check the file request status every time. if the data owner response their request they get the file key and download the file.

6. Download Details

In this module, cloud can view all download file information from the server. data owner and data user both are download the file from server after file decryption process.

SYSTEM ARCHITECTURE



Encryption technologies have become one of the most prevalent solutions to safeguard data confidentiality in many real-world applications, e.g., cloud-based data storage systems. Encryption outputting a relatively “static” format of encrypted data, however, may hinder further data operations. For example, encrypted data may need to be “transformed” into other formats for computation or other purposes. To enable encryption to be used in another device equipped with a different encryption mechanism, the concept of encryption switching was first proposed in CRYPTO 2016 for conversion particularly between Paillier and ElGamal encryptions.

OPERATIONAL EXPENDITURE

We secure the content using two encryption switching protocol IBE and ABE.

4. CONCLUSION

We have conclude the process are in encryption switching between ibe and abe which is the first of its type in the literature. The security notion has been defined in the game based framework. We have presented a concrete construction and meanwhile proved it to be cpa secure in the standard model under the decisional q-parallel bdhe assumption. The efficiency analysis has highlighted that our solution outperforms the download-and-re-encrypt conversion mode w.r.t. Computation and communication cost. At last, the simulation results have shown that the computational complexity in terms of re-encryption and decryption (in our construction) are in the acceptable range, e.g., around 0.9 s and 2.5 s for abe!ibe re-encryption and decryption, respectively. Some interesting open problems have been incurred from this work as well, for example, how to shorten the re-encrypt and decrypt time at the case of abe!ibe, and seek an approach to achieve simulation-based security.

REFERENCES

[1] G. Couteau, T. Peters, and D. Pointcheval, "Encryption switching protocols," in Advances in Cryptology - CRYPTO 2016 - 36th Annual International
Cryptology Conference, 2016, Proceedings, Part I, ser. Lecture Notes in Computer Science, M. Robshaw and J. Katz, Eds., vol. 9814. Springer, 2016, pp. 308–338.

[2] P. Paillier, "Paillier encryption and signature schemes," in Encyclopedia of
Cryptography and Security, 2nd Ed., H. C. A. van Tilborg and S. Jajodia, Eds. Springer, 2011, pp. 902–903.

[3] A. Shamir, "Identity-based cryptosystems and signature schemes," in
Advances in Cryptology, Proceedings of CRYPTO '84, 1984, Proceedings, 1984, pp. 47–53.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption
for fine-grained access control of encrypted data," in ACM CCS'06, 2006, pp. 89–98.

[5] M. Portnoi and C. Shen, "Secure zones: An attributebased encryption advisory system for safe firearms," in IEEE Conference on Communications and Network Security, CNS 2013, 2013. IEEE, 2013, pp. 397–398. [Online]. Available:
https://doi.org/10.1109/CNS.2013.6682746

[6] T. Mizuno and H. Doi, "Hybrid proxy re-encryption scheme for attributebased encryption," in Information Security and Cryptology - 5th

International Conference, Inscrypt 2009, 2009. Revised Selected Papers, 2009, pp. 288–302.

[7] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, 2001, Proceedings, 2001, pp. 213–229.

[8] D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," in Advances in Cryptology - CRYPTO 2004, 24th Annual International Cryptology Conference, 2004, Proceedings, 2004, pp. 443–459.

[9] B. Waters, "Efficient identity-based encryption without random oracles," in Advances in Cryptology - EUROCRYPT 2015.

[10] C. Gentry, "Practical identity-based encryption without random oracles," in Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2006, Proceedings, 2006, pp. 445–464.

[11] C. Fan, L. Huang, and P. Ho, "Anonymous multireceiver identity-based
encryption," IEEE Trans. Computers, vol. 59, no. 9, pp. 1239–1249, 2010.

[12] X. Boyen and B. Waters, "Anonymous hierarchical identity-based encryption (without random oracles)," in Advances in Cryptology – CRYPTO 2006, 26th Annual International Cryptology Conference, 2006, Proceedings, 2006, pp. 290–307.

[14] J. Kim, W. Susilo, M. H. Au, and J. Seberry, "Adaptively secure identitybased broadcast encryption with a constant-sized ciphertext," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 679–693, 2015.