Journal of Engineering and Applied Sciences 12 (Special Issue 4): 6733-6734, 2017
ISSN: 1816-949X

Secure and Efficient Data Sharing with Third Party Re-Encryption in Cloud Storage

[1]A. Vinay and [2]S. Natarajan
[1]Department of Information Technology, AMET University, Chennai, India
[2]Department of Computer Science, PES Institute of Technology, Bangalore, India

Abstract: Data sharing and large acceptance of cloud computing is rapid development in cloud storage. The guarantee of the customer's data protection is becoming that delay wide acceptance of cloud computing. To secure data sharing of cloud computing is talented explanation of third party re-encryption. A data holder to encrypt distributed data in cloud storage to permits under its individual public key which is changed by a semi-trusted cloud server into a planned encryption for the genuine beneficiary for access control. This study provides a solid and inspirational review of third party re-encryption from dissimilar perspectives to recommend an improved accepting of this primitive. In exacting, the third party re-encryption is evaluated by observing the protection methods and the intend philosophy. In addition, the possible applications and additions of third party re-encryption have also been conversed.

Key words: Cloud computing, data protection, third party re-encryption, public key, access control, possible

INTRODUCTION

Third party re-encryption permits to transform a cipher text calculated under Alice's public key into one that can be unlocked by Bob's secret key. Not including Bob's secret key, to forward encrypted mail to Alice co-worker Bob (Lee *et al*., 2010). In this case, Alice the delegator could assign a third party to re-encrypt her received mail into a design that Bob the delegate can decrypt using his individual secret key. Alice could basically offer her secret key to the third party but this entails an impracticable stage of trust in the third party (Xiong *et al*., 2012).

Third Party Re-Encryption (TPRE) enables a semi-trusted server to transform a cipher text of encrypted data under the public key of delegator into cipher text under the public key of delegatee without disclosing the primary encrypted messages of delegator/delegatee to the third party. The guarantee of the customer's data protection is becoming that delay wide acceptance of cloud computing (Yang *et al*., 2011). To share sensitive data stored in cloud storage from data holder (say, Alice) to another approved user (say, Bob). Encouraged by the primitive of TPRE, Alice using own public key can encrypt the sensitive data before uploading the shared data to the semi-trusted cloud server. After receiving the data sharing request from Bob, Alice produces a third party re-encryption key using her own private key and Bob's public key and mails this third party re-encryption key to the semi-trusted cloud server. Third party re-encryption key, cloud server can transform the encrypted cipher text with public key of Alice into an encryption under the public key of Bob (Ateniese *et al*., 2005). By utilizing the TPRE primitive, the received by bobs cipher text can only be decrypted by him while the cloud server is incapable to learn the plaintext or private keys of Alice or Bob. In conclusion, decrypt and download the received data with Bob's private key (Ateniese and Hohenberger, 2005).

Literature review: In their general construction of proxy signature is Bob's signature is observed as a double signature which contains a signature from Alice and one from the proxy. There is no conversion between suitable Alice's signatures into Bob's ones and Alice's signing secret key is actually provided to her by Bob (or by a trusted authority) (Libert and Vergnavd, 2008). A general structure for protection mediated certificateless encryption which offers instant revocation. An outstanding investigation of certificateless encryption provides ranks and methods, the dissimilar concepts of protection for a certificateless public key encryption method against an outside attacker as well as passive key generation center in survey on encryption techniques used to secure cloud storage system (Kirubakaramoorthi *et al*., 2015).

The CCA secure ID based proxy re-encryption method without random oracles. The ciphertext complexity and size of the decryption algorithm grew linearly in the amount of transformations done to a ciphertext. A CCA

Corresponding Author: A. Vinay, Department of Information Technology, AMET University, Chennai, India

secure multi-hop ID based proxy re-encryption scheme in the usual model having constant computational and ciphertext complexity and Generating a digital signature based on new cryptographic scheme for user authentication and security (Ganeshkumar and Arivazhagan, 2014). Proxy re-signatures can be used as an alternative to multi-signatures but not to collective signatures, given that we permit transformations to be through only between signatures on the same message.

MATERIALS AND METHODS

To overcome the above mentioned security problems we are implementing the third party re-encryption. The definition of a unidirectional TPRE method consists of the following polynomial time algorithms: KeyGenerate, ReEnKey, Signature, ReSignature and Verify.

KeyGenerate: Input of security parameter kϵK, user b runs this algorithm to produce its public/private key pair (pkb, skb).

ReEnKey: Input of key pair (pkb, skb) for user v and a key pair (pkv, skv) for client q (skv is optional), the re-encryption key generation algorithm ReEnKey is achieved by user b to output a re-encryption key rkb$\neg$v. Since, the re-encryption key rkb$\neg$v allows transforming user b's signature into user v's signature, thus user q acts as the delegator and user b acts as the delegate.

Signature: Input of message mϵM and its own private key skb, user b executes this algorithm to calculate a corresponding signature σb.

ReSignature: Input of a signature σb from user b and a re-signature key rkb$\neg$v, this algorithm is performed by the third party to produce a re-signed signature σb$\neg$v, if Verify(pkb, m, σb) = 1 holds; Otherwise, this algorithm returns an error symbol $\perp$ indicating σb is invalid.

Verify: Input of a public key pkb of user b, the message mϵM and an equivalent signature σb, a verifier achieves this algorithm to ensure the validity of this signature. If Verify (pkb, m, σb) holds, it returns 1; otherwise, returns 0.

RESULTS AND DISCUSSION

The delegate or delegator is aware of the existence of the proxy. It is unfeasible for any delegate to differentiate an original encryption calculated under his public key using the Encrypt algorithm from a re-encryption ciphertext on the similar message produced by the third party as the production of the ReEnKey algorithm. The input and the equivalent output of the ReEnKey algorithm in the transparent PRE method cannot be linked to each other.

CONCLUSION

In cloud computing, to protect the data sharing, Third Party Re-Encryption (TPRE) has a set of anxiety due to the delegation function of decryption. We evaluated the art of the Third Party Re-Encryption (TPRE) by comparing the effectiveness of previous methods, investigative the safety models and investigative the design attitude.

REFERENCES

Ateniese, G. and S. Hohenberger, 2005. Proxy re-signatures: New definitions, algorithms and applications. Proceedings of the 12thComputer and Communications Security, Nov. 7-11, USA, pp: 310-319.

Ateniese, G., K. Fu, M. Green and S. Honhenberger, 2005. Improved proxy re-encryption schemes with applications to secure distributed storage. Proceedings of the NDSS, February 3-4, 2005, The Internet Society, pp: 29-43.

Ganeshkumar, K. and D. Arivazhagan, 2014. Generating a digital signature based on new cryptographic scheme for user authentication and security. Indian J. Sci. Technol., 7: 1-5.

Kirubakaramoorthi, R., D. Arivazhagan and D. Helen, 2015. Survey on encryption techniques used to secure cloud storage system. Indian J. Sci. Technol., Vol. 8, 10.17485/ijst/2015/v8i36/87861

Lee, S., H. Park and J. Kim, 2010. A secure and mutual-profitable DRM interoperability scheme. Proceedings of the 2010 IEEE Symposium on Computers and Communications (ISCC'10), June 22-25, 2010, IEEE, Riccione, Italy, ISBN:978-1-4244-7754-8, pp: 75-80.

Libert, B. and D. Vergnaud, 2008. Unidirectional chosen-ciphertext secure proxy re-encryption. Proceedings of the PKC 2008, March 9-12, 2008, Springer Berlin/Heidelberg, pp: 360-379.

Xiong, H., Z. Chen and F. Li, 2012. Efficient privacy-preserving authentication protocol for vehicular communications with trustworthy. Secur. Commun. Netw., 5: 1441-1451.

Yang, T., H. Xiong, J. Hu, Y. Wang and W. Xin et al., 2011. A traceable privacy-preserving authentication protocol for VANETs based on proxy re-signature. Proceedings of the 2011 IEEE 8th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD'11) Vol. 4, July 26-28, 2011, IEEE, Shanghai, China, ISBN:978-1-61284-180-9, pp: 2217-2221.