Efficient privacy preserving scheme for cloud computing

Dr. Mani Arora

Khalsa College,Amritsar

Abstract:

In recent years, worldwide cloud computing has been acclaimed due to its conceptual and infrastructural foundation. Resource pooling and large network access are the most important features of its gradual growth. Hike in data generated and stored on cloud servers is exponential. In it the data is controlled by third party who poses a main security threat. This paper presents a concise survey of existing asymmetric encryption techniques used to secure data in transmission in cloud computing and outline the efficient privacy preserving encryption technique

Keywords: Cloud server, encryption, asymmetric, cloud security, cryptography, metrics

Introduction

In the present system, at global level cloud computing is an upcoming realm that focused on protected "services" provided to clients on demand basis. Numerous commercial clients save immense data on cloud. Ever since the cloud computing emerged, vast amount of data is being intense on the cloud. Due to the stocky data being transferred on cloud its need of an hour to protect data from unethical hackers and attackers. Major threat to cloud data is when third party controls the connections between owner of data and cloud service provider. To manage security challenges, a number of research works have been carried out and various encryption techniques have been developed. In this segment we have sketched some parameters which can be used to analyse and evaluate various asymmetric encryption algorithms used to secure data in transmission.

The following are the parameters which can be used to evaluate various security algorithms

1. Cipher text size: The size of text produced after encryption
2. Confidentiality: Any offender should not able to fetch any information about encrypted files.
3. Efficiency: An encryption algorithm is considered to be efficient if its computational cost is below some tolerable point.
4. Flexibility: An encryption algorithm can be executed sequentially or in parallel producing cipher text independent of platform and execution order.
5. Scalability: The ability of an algorithm to be used or produced in the range of capabilities
6. Access control: It is a novel paradigm for encryption which allows controlling not only what users in the system are allowed to read but also what they are allowed to write.

Overview of Encryption Algorithms

The asymmetric encryption techniques have assorted characteristics in overseeing data transmitted to cloud servers such as identity based encryption, functional encryption, verifiable computation(VC), homomorphism encryption (HE), attribute based encryption as well as secure multiparty computation(MPC).There is also available Advanced encryption standard(AES), Format Preserving Encryption(FPE) based on symmetric key encryption. An analogous technique is Format Preserving Hashing (FPH) performing secure hashing .

AES

Advanced Encryption standard (AES) is a broadly adopted symmetric encryption algorithm which converts plain text into cipher text at least six time faster than triple DES [1]. It uses the same private key to encrypt and decrypt data. AES is an iterative cipher rather than Feistel cipher [2]. It is based on 'substitution–permutation network' method. It encompasses four main operations, two of which demand replacing inputs by specific outputs (substitutions) whereas others two shuffle bits around (permutations). AES perform all computations on bytes relatively than bits. It treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four rows as well as four columns for dealing out as a matrix. AES encrypt data in 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a 128-bit round key, which is calculated from the original AES private key [3]. The cipher text size is same as that of plain text size so no extra vulnerability in bandwidth of transmission links. The data owner firstly encrypts data using AES and then transmit it to cloud server using SSL (Secure socket layer).SSL is used to protect data while transmission from one end to other. The above approach taken by Prabhakar and Joseph [4] provides end to end security of data during transmission in the cloud environment. They divided the whole process in two stages. In stage 1 data is encrypted using AES technique. Stage 2 deals with data retrieval and decryption. In both stages data remains encrypted so cloud provider has no knowledge of the key so data confidentiality is guaranteed .However a major drawback is efficiency and access control.

Format Preserving Encryption

It is exceedingly fast symmetric encryption technique as it is based on block ciphers. It encrypts a plaintext of some specified format into a cipher text of the same format and size. It employs basic symmetric encryption techniques including AES. It uses Fiestal network .Fiestal network uses the round function to preserve format [5]. It is relatively appropriate for

encrypting data as well as grants confidentiality however its analytics capabilities are limited; yet very undemanding queries might need re-encryption.

Homomorphic Encryption

In it the algebraic manipulation like multiplication and addition are done on plaintext. This type of encryption has been in existence from the time when the public key cryptography [6] initiated. In [7] a scheme is proposed to perform algebraic query processing over encrypted data. It focuses on protecting data during all stages of the sharing process. The four stages are Evaluate algorithm, KeyGen, Encrypt and decrypt algorithms. However the issues regarding user authentication and building indexes is not properly dealt with.

Identity based Broadcast Encryption

It was anticipated in 1994[8]. In it the data broadcaster or sender encrypts the data file and furthermore it was sent to the group of users. The receivers then use their private key to decrypt the message. The sender opts for a set of uniqueness at the encryption step, so that only the proposed users are dexterous to decrypt the transmitted file. Hierarchical Identity based Encryption is used to restrict users who are unauthorized or partially authorized and might share their key with some unauthorized users which will escort to unauthorized data access[9][10] .It consist of five main operations Setup Encrypt, KeyGen, Decrypt and Delegate. In the initial step the authorized person runs the setup algorithm to get public key and private key. Then in next step user runs encryption algorithm to encrypt data before transmitting to cloud server. In next step user runs query algorithm to generate query and finally decryption algorithm is used to decrypt cipher text. In this scheme some stages take more time if number of users increase.

Attribute based Encryption

It is again asymmetric encryption technique which is proposed in 2005.In this encryption technique the private key of a user and the cipher text are dependent upon attributes (e.g. the country in which he lives, or the kind of subscription he has). It is most suitable for multi owner data .In it, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the cipher text. The scheme presented in [11] focus on sharing data in multi owner manner .It again based on concept of firstly encrypting data and

then transmitting it to cloud. There are primarily two types of attribute-based encryption schemes: Key-policy attribute-based encryption (KP-ABE)[12] and cipher text-policy attribute-based encryption (CP-ABE)[13].In KP-ABE, users' private keys are made-up based on a right to use tree that classifies the privileges allowed to concerned user, and data are encrypted over a set of attributes. However, CP-ABE uses access trees to encode data and users' furtive keys are generated over a set of attributes. Attribute-based encryption methods are also extensively employed in vector-driven search engine interfaces.

Proxy re-encryption

It was projected in 1998 to facilitate re-encryption of some cipher text encrypted by one user such that an additional user will be able to decrypt it. It is predominantly useful in cases when one user wants to forward some encrypted data on cloud to an added user without the need of key forwarding. It is used on top of ABE schemes. Data sharing scheme proposed in [14] is both secure and efficient based on proxy re-encryption united with homomorphic encryption. This technique consists of five steps key generation and distribution in which data owner create and distributes a pair of keys to system users, Data outsourcing in which the data owner encrypts the data and generate token for each file, Data access in which cloud service provider checks authorization of user requesting access to data and take appropriate action accordingly, User revocation where owner of data evocate user’s access rights and User rejoin in which data owner issue new token to the user with access rights.

Verifiable Computation

This technique is primarily used for dealing out big data in private clouds. It allocates data owner to verify the integrity of the computation. The data owner sends the data along with a pattern of the computation desired. The computation systems then output the outcome of the specified computation along with some influential argument or verification that this data is in fact correct and the data receiver verifies the proof.

Conclusion

Cloud computing is the most emerging technology and security of data during transmission is the most important concern .This demands that most efficient privacy preserving scheme should be used to secure data on cloud as well as data in transmission. We have outlined some most demanding techniques in above section in which we try to project out how encryption is used for securing data. If we compare the above techniques on the basis of parameters discussed in beginning of paper then the techniques which provide and fulfil most

security requirements are Homomorphic Encryption and Attribute based Encryption. In the future work , will propose a scheme that will contain the security features of both encryption techniques.

References

[1] A. Tripathi, M.S. Jalil, **Data access and integrity with authentication in hybrid cloud** Orient. International J. Innovative Engrg. Res., 1 (1) (2013) 030

[2] Rijndael (1998) " Rijndael AES proposal " *National institute of science and technology*. Available [online] http://www. Csrc.nist.gov/encryption/aes/.

[3] Awadhesh Kumar and R.R. Tewari "Expansion of Round Key Generations in Advanced Encryption Standard for Secure Communication" International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 13, Number 7 (2017), pp. 1679-1698

[4] D.M. Prabhakar, K.S. Joseph, A new approach for providing data security and secure data transfer in cloud computing.

[5] Nilekh Chaudhari, "A CLOUD SECURITY APPROACH FOR DATA AT REST USING FPE" International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol. 5,No. 1, February 2015

[6] M.G. Kaosar, R. Paulet, X. YiFully homomorphic encryption based two-party association rule mining Data Knowl. Eng., 76 (2012), pp. 1-15

[7] M. Mani, K. Shah, M. Gunda, Enabling secure database as a service using fully homomorphic encryption: Challenges and opportunities. arXiv preprint, 2013. arXiv:1302.2654

[8] A. Fiat, M. Naor Broadcast encryption Advances in CryptologyCRYPTO93, Springer (1994), pp. 480-491

[9] J.H. Seo, J.H. Cheon, Fully secure anonymous hierarchical identitybased encryption with constant size ciphertexts. IACR Cryptology ePrint Archive, 2011:21, 2011.

[10] J. Baek, J. Newmarch, R. Safavi-Naini, W. Susilo, A survey of identitybased encryption, 2005.

[11] X. Liu, Y. Zhang, B. Wang, J. Yan, Mona: secure multi-owner data sharing for dynamic groups in the cloud, IEEE Trans. Parallel Distrib. Syst. 24 (6) (2013) 1182–1191.

[12] Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters, Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data ACM CCS (2006)

[13] *Bethencourt, J.; Sahai, A.; Waters, B. (2007-05-01). Ciphertext-Policy Attribute-Based Encryption. 2007 IEEE Symposium on Security and Privacy (SP '07). pp. 321–334* doi:10.1109/SP.2007.11. ISBN 978-0-7695-2848-9.

[14] B.K. Samanthula, G. Howser, Y. Elmehdwi, S. MadriaAn efficient and secure data sharing framework using homomorphic encryption in the cloud .In Proceedings of the 1st International Workshop on Cloud Intelligence, ACM (2012), p. 8