Encryption Techniques to Ensure Data Confidentiality in Cloud

V. Reena Catherine, A. Shajin Nargunam

Abstract**:** ***Cloud computing is proving to be a beneficial model for all types of users as it enables anyone to share and make use of the available pool of resources and get the desired services online. It reduces the operational and maintenance costs since the user needs to pay for what he has used. Databases and applications are moved to the cloud and stored in large data stores of the cloud service provider which may be insecure or untrustworthy. End users want to know the location of data being stored and who have control over the information apart from the owners. They particularly want the data to be secured from unintentional or illegal access even by the service providers. As the data are stored in geographically dispersed area, the data is vulnerable. The most important concern is that data confidentiality is to be attained while data is stored or in transit. To provide confidentiality, initially cryptographic approaches were used that disclose the keys needed for decryption only to the authorized users. But in the cloud, the adopted encryption schemes should support fine-grained access control, high performance, scalability as well as full delegation. In order to share valuable data confidentially on the cloud in a secured way, various encryption techniques are available starting from Identity-Based Encryption, Attribute-Based Encryption, Hierarchical Attribute-Based Encryption, Identity-Based Broadcast Encryption, Searchable Encryption, Homomorphic Encryption, Fully Homomorphic Encryption and so on. This paper analyses some of the recent and popular encryption techniques and discusses the issues related to them.***

Keywords— Cloud computing, confidentiality, encryption techniques.

I. INTRODUCTION

The usage of online trading and e-commerce is drastically expanding each and every day. This internet-based computing is called cloud computing as the computing details are hidden from the users just like a cloud hides what is beyond it. From the definition given by the NIST, it is well understood that cloud computing offers convenient access to the available shared pool of resources whenever there is a demand. It supports rapid elasticity and needs only a few interactions with the service provider. The resources may be applications, services, servers, storage and networks [1].According to the ownership and usage, a cloud can be classified into four categories, namely private, public, community and hybrid clouds. Infrastructure, Platform and Software can be delivered as-a-Service. Based on the service rendered, a cloud can be categorized as IaaS, PaaS and SaaS. Usually, due to resource limitations and availability issues, the owner of a data prefers to move the content to the cloud. When the data is moved to the cloud, he / she loses control of data. He has to entrust its security to the Cloud Service Provider (CSP). But there is no guarantee that the data is not maliciously attacked by others or the CSP is accessing the data illegally. In order to make use of the cloud with trust, the major concern for security is data confidentiality and privacy.

Confidentiality refers to the ability to access the protected data only by the authorized parties. Data confidentiality could be breached due to the cloud characteristics such as multitenancy, object reusability and data remanence.

The two major consequences of shifting data storage and IT infrastructure to the cloud entrusting third-party providers [2]:

(a) As the data owners have limited control, proper security policies must be enforced for ensuring data confidentiality and integrity;

(b) Cloud service providers have more privileges and can easily control and modify the IT systems and data of the users.

Security requirements for secure data storage in the cloud [3]:

- Data stored in the cloud are to be kept confidential and the cloud storage provider must be prevented from intruding.
- Only the data owner should have the authority to share the data. The data owner decides on the data user.
- Other than the privileged user, no one can access the data including the cloud provider.

Attempting to illegally access the data available on the cloud is increasing exponentially. Encryption keeps the data secure, but it becomes useless if the keys are lost. Therefore, it becomes necessary to develop and use various cryptographic techniques [4], [5] that can safeguard the data from both active and passive attacks. So the first step for ensuring data confidentiality is to encrypt the data and then send it to the cloud. But we may need to perform various computations on the encrypted data while still in cloud. For this purpose various techniques for encryption are used in the cloud.

Revised Manuscript Received on September 22, 2019.

V. Reena Catherine, 1Research Scholar in Computer Science, Noorul Islam Centre for Higher Education,Kumaracoil, India. Email:reenavargheese11@gmail.com

A. Shajin Nargunam, 2Director /Academic Affairs,Depatment of CSE, Noorul Islam Centre for Higher Education,Kumaracoil, India

Retrieval Number: K121509811S19/2019©BEIESP
DOI: 10.35940/ijitee.K1215.09811S19

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Section II introduces the various encryption techniques used in the cloud and their related work. Section III discusses encryption techniques and their advantages and limitations. Section IV concludes this survey paper and suggests the direction for proceeding with further research.

II. RELATED WORK

Confidentiality refers to preventing any data (trivial as well as critical information) from access (intentional or unintentional intrusion) and at the same time ensuring that the data is accessible only to the authorized users. Data must be encrypted and then stored in the cloud because the cloud cannot be trusted all the time.

Various cryptographic approaches have been used to ensure data confidentiality. Yu et al. [6] have used attribute-based encryption, which is based on a set of attributes of the user and an access policy. Based on their association with private key and ciphertext, ABE is of two types, namely Ciphertext Policy Attribute-Based Encryption (CP-ABE) [7] and Key Policy Attribute-Based Encryption (KP-ABE) [8]. Operations can be performed on encrypted data itself in Fully Homomorphic Encryption [9] and Searchable Encryption [10, 11, 12]. Attribute-Based Signatures are introduced that can be combined with Encryption and termed as Attribute-Based Signcryption. ABS maintains anonymity of the signer, as the identity of the signer is not revealed. Also outsourcing of designcryption process and signer verification is added in CP-OABSC scheme which is proposed by Deng et al. [16] Based on these works, a wide range of researchers and academicians are brainstorming and coming up with many innovative and efficient encryption schemes.

III. ENCRYPTION TECHNIQUES

This section discusses on the various encryption techniques used in the cloud for security purpose along with their advantages and limitations.

A.Traditional Encryption Methods

The traditional encryption methods like symmetric encryption and public key encryption are numeric key based techniques. Only the key holder can encrypt and decrypt and so other unauthorized users cannot gain access to the data. These methods are useful to secure data, but data loss can be disastrous when the keys become exposed. Users cannot perform operations on the encrypted data, i.e. the ciphertext.

B. Identity-Based Encryption (IBE)

IBE uses a unique information of the user like email id as the public key for encryption. Therefore the encryption process is much easier when compared to other techniques. Using the IBE technique, it is easy to encrypt as the user's public key is common knowledge, but data loss can be disastrous when the decryption key become exposed. Here also users cannot perform operations on the encrypted data.

C. Identity-Based Broadcast Encryption (IDBBE)

In this method, the data owner can encrypt the data once and then can broadcast the data in encrypted form to a selected group of users. The set of identities of the receivers is used for encryption. IDBBE enables one-to-many communication and reduces computation as the data need to be encrypted only once, but users cannot perform operations on the encrypted data.

D. Attribute-Based Encryption (ABE)

This technique is a type of public-key encryption. A set of attributes of the user is used as the secret key and for decryption [6]. In ABE, decryption can be done, if and only if the set of attributes of the user key and the attributes of the ciphertext match with each other. Users cannot perform operations on the encrypted data. Security can be enhanced when the number of attributes involved is more.

E. Ciphertext Policy Attribute-Based Encryption (CP-ABE)

The private key is based on attributes of the user and is issued by a Central Authority. Using the attributes and logic gates, a tree is formed which is called the access policy. For a user to decrypt, his attributes must satisfy the access policy [7]. In CP-ABE, security is enhanced than the previously mentioned techniques. But, it needs a Central Authority to issue the key. Users cannot perform operations on the encrypted data.

F. Key-Policy Attribute-Based Encryption (KP-ABE)

It is the opposite of CP-ABE. The private key is based on access policy and ciphertext is associated with a set of attributes [8]. KP-ABE method is useful for authentication. But, it is not as secure as CP-ABE and users cannot perform operations on the ciphertext.

G. Hierarchical Attribute-Based Encryption (HABE)

HABE combines both Hierarchical Identity-Based Encryption and CP-ABE [6,14]. HABE is useful to achieve fine-grained access control. It needs public key generators to generate and distribute keys and system parameters, and also to authorize top level domain authorities in the hierarchy. Users cannot perform operations on the data in the encrypted form.

H. Fully Homomorphic Encryption (FHE)

FHE enables computations to be performed on the encrypted data and operations like sum and product can be done without decryption [9, 15]. Even though FHE allows operations to be performed on encrypted data, but the search operation cannot be done. Also, the computation overhead is more.

I. Searchable Encryption (SE)

SE enables keyword search on encrypted data. Builds a keyword index to answer the search queries [10,11,12]. SE is useful to provide results for top-k searches and to provide results based on ranking. But, it suffers from information and privacy leakage as the cloud server can find out size, search and access patterns.

J. Attribute-Based Signature (ABS)

ABS enables to sign a message without the need to expose the identity of the signer. It allows the user to sign only when his set of attributes matches the set of attributes and predicate mentioned by the authority. ABS is useful to sign a message anonymously. It denotes that some user whose attributes satisfy the predicate has signed yet his true identity is not revealed.But, large computational overhead is needed for signing.

K. Attribute-Based Signcryption (ABSC)

In this technique, signing and then encryption is done by the sender. Signing attributes are different from the decryption attributes. It achieves confidentiality and authenticity simultaneously. The ciphertext is unforgeable. But, a high computational cost is incurred to the user as there is an increased computational overhead to the user.

L. Ciphertext Policy Attribute-Based Signcryption (CP-ABSC)

Signing and then encryption based on CP-ABE is done by the sender in CP-ABSC. It achieves confidentiality, privacy of the signer, fine-grained access control, verifiability and authenticity simultaneously. But, he computational cost is high for the users.

M. Ciphertext Policy Attribute-Based Signcryption with Outsourced Designcryption (CP-OABSC)

In CP-OABSC, the decryption process is outsourced and the signature can be verified [16]. It reduces the computation cost of the user. Also, it is useful even when the cloud server is not trusted worthy. But, there is an increased computational overhead for the server since the decryption and verification operation is done at the cloud server.

N. Order Preserving Encryption (OPE)

OPE preserves the order of ciphertext with that of the plaintext [13]. OPE is suitable for sorting operations. Also, it shows moderate leakage. But, a lot of computation is needed.

O. Time Release Encryption (TRE)

TRE enables to encrypt time sensitive data which can later be released by different users as given permission [14, 19]. In TRE, data dissemination based on time is allowed thus reducing the burden on the data owner for sending data to designated users at different time.

IV. RESULT AND CONCLUSION

The usage of the cloud and its services are becoming almost inseparable in almost all our day-to-day activities. The cloud characteristics like resource sharing, on-demand self-service, metered service, fast and desired elasticity attract every single internet user to become the cloud users and yet the characteristics like geographic distribution and multitenancy arises security issues like data confidentiality and privacy. In this paper, we have presented an overview of the various encryption techniques that are quite promising in providing data confidentiality. The various techniques are compared that gives us a clear view on how to choose the needed encryption scheme to suit our requirement in the cloud. From the observation, it is understood that the existing encryption techniques are having heavy computational overhead and so the computation cost is high and also most techniques do not provide efficient operations to be done on encrypted data. Therefore, further research is to be done that not only provides confidentiality, verifiability but also allows operations to be carried out on encrypted data and thus reducing the computational cost.

REFERENCES

1) National Institute of Standards and Technology. The NIST definition of cloud computing; 2011. <http://www.nist.gov/itl/cloud/upload/cloud-defv15. pdf> [retrieved 24.09.18].

2) Rong Chunming, Nguyen Son T. Cloud trends and security challenges. In: Proceedings of the 3rd international workshop on security and computer networks (IWSCN 2011); 2011.

3) Rong C et al. Beyond lightning: A survey on security challenges in cloud computing. Computers and Electrical Engineering(2012). http://dx.doi.org/10.1016/j.compeleceng.2012.04.015.

4) Wang Z, Sun G, Chen D. A new definition of homomorphic signature for identity management in mobile cloud computing, Journal of Computer and System Sciences, Vol. 80, N0. 3, 2014, pp. 546-553.

5) Yakoubov S, Gadepally V, Schear N, Shen E, Yerukhimovich A. A Survey of Cryptographic Approaches to Securing Big-Data Analytics in the Cloud, IEEE High Performance Extreme Computing Conference (HPEC), 2014, pp. 1–6.

6) S. Yu, C. Wang, K. Ren and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in Proc. 29th Conference on Information Communications, San Diego, CA, USA, 2010, pp. 534-542.

7) J. Bethencourt, A. Sahai and B. Waters, “Ciphertext-policy attribute-based encryption,” in Proc. 2007 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2007, pp. 321-334.

8) N. Attrapadung, B. Libert, and E. De Panafieu, “Expressive key-policy attribute-based encryption with constant-size ciphertexts,” in Public Key Cryptography–PKC 2011. Springer, 2011, pp. 90–108.

9) Wei L, Zhu H, Cao Z, Dong X, Jia W, Chen Y, Vasilakos AV. Security and privacy for storage and computation in cloud computing, Information Sciences, Vol. 258, 2014, pp. 371-386.

10) D. Song, D. Wagner, and A. Perrig, “Practical Techniques for Searches on Encrypted Data,” in Proc. of IEEE S&P’00, 2000.