International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 11, 2019 (Special Issue)

A Survey of Encryption techniques in cloud computing

Mrs.J.Nithisha
Assistant Professor ,
Department of Information Technology ,
Jeppiaar Engineering College,
Chennai,India

Abstract— ***Cloud Computing is very flexible in nature it helps to quickly access the resources efficiently from the third party service provider with low cost. A cloud storage system allows us to stores huge amount of data in its storage server. Since the data is stored in the server for a long time over the internet it does not provide any confidentiality of data .The hackers may steal the data from the storage system and also when data forwarded to cloud environment.So data integrity is violated. Inorder to main the integrity and security we need to encrypt the data. In this paper discussed about different encryption technique to protect the data in the cloud***

Keywords— Cloud, protected data, encryption, decryption

.

I.INTRODUCTION

Cloud computing is emerging technology for sharing resources which include infrastructure, software, and applications processes. Cloud computing architecture provides computing service through the internet on demand and allows user to access shared resources like networks, storage, servers, services and applications. Cloud computing allows the user to store large amount. Cloud provides high speed data transfer services through the internet. Cloud provides users to collect data or share data from anywhere through internet. Cloud computing allows multiple users to access different operations on their data. Cloud also provides high speed services with low cost. Cloud provides users to access the data on cloud remotely. Cloud Service provider provides service to the customer who can easily recover hacked or lost. And also by using encryption technique, it provides data authentication and security so that user does not face any issues like data loss or data theft.

A. Service models in cloud computing

Cloud service categories are software as-a-service (SaaS), platform-as-a-service (PaaS) and infrastructure-as -a-service (IaaS).

- IaaS –. IaaS is one of the three main categories of cloud computing services, Infrastructure as a service (IaaS) is a form of cloud computing that provides that are used to maintain and monitor the cloud data, network or networking services.
- PaaS – Platform as a service Cloud platform services provide runtime development and deployment tools that are used in the development of applications
- SaaS – software as-a-service model allows to use software applications as a service to end-users and used to manage third party software .Using SaaS,the applications can run directly without downloads or installation

B.Cloud Deployment model

Four different cloud deployment models are used such as public cloud, private cloud ,hybrid cloud and community cloud

Public Clouds

It is one of the common type of cloud deployment model. Customers use the services offered by cloud service providers. The companies like sky drive, Google drive and iCloud services uses this type of deployment model. Customers do not know about the infrastructure and working of the computing mechanism. Consumers can add or retrieve the data at any moment as required.

Private Clouds

Large companies and enterprises uses this type of cloud as it gives private environment for storage and they can use the security measures which is suited for them. The cost of deploying private cloud is high. This type of service used in the area where privacy is main concern. Many banks use private cloud to provide private services to customers and employers.

Hybrid Clouds

This type of deployment is used where we need both the private and public deployment model simultaneously. The security strategies are mostly independent for both type of services. The cost required is less as both models are integrated in one system. Best example of this model is Amazon's simple storage service.

Community Cloud

More than one single infrastructures are used by this type of model. More than one organizations can control service deployment model. The control may be administered by more than a single provider. Used when many organizations may have a shared interest to use a single cloud model.

II.RELATED WORK

- In Cloud Storage, any organization's or individual's data can be stored in and accessible from multiple distributed and connected resources or locations that comprises cloud. To provide secured communication over distributed and connected resources, encryption algorithms plays a vital role. It is the basic tool or method for protecting the data. Encryption algorithm converts the data into scrambled form by using "key" and only authorized user have the key to decrypt the data. In

Symmetric key encryption, one key is used to encrypt and decrypt the data. Another technique is known as asymmetric key encryption in which two keys-private and public keys are used. Public key is used for encryption and private key is used for decryption .User's data can be made secured in the cloud using encryption

III SECURITY SERVICES

A security services as a service provided by a protocol layer of communicating open system, which ensures adequate security of the system or of data transfer.

Authentication: The assurance that the communicating entity is the one that it claims to be.

Access control: The prevention of unauthorized use of a resource.

Data confidentiality: It is the protection of transmitted data from passive attacks.

Data integrity: The assurance that data received are exactly as sent by an authorized entity that is it contain no modification, insertion or deletion.

Non-Repudiation: It prevents either sender or receiver from denying a transmitted message.

IV .SECURITY ISSUES IN THE CLOUD

Despite cloud computing have many benefits,security is the main concern. Data store on the cloud lacks it security as it can travel through internet and accessed by other. There are many security issues in cloud computing as it uses various resources like operating system ,networks and databases. Thus, security issues for these and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. virtualization in cloud computing results in many security issues. For example, mapping of virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as security policies used to secure data. Resource allocation and memory management algorithms also to be secure.Finally need to find the malware detection in clouds. .In order to secure the resources shared in cloud we need to implement security measures like encryption techniques.

V CRYPTOGRAPHIC TECHNIQUES

The main aim of cryptographic technique is to provide secure data in cloud.There are many encryption technologies used . In earlier days most common encryption Technique like Public Key Encryption technique was applied. This method does not provide expected result as it supports one to one encryption so it is not scalable. So some advanced techniques used for encryption.

- Identity Based Encryption
- Attribute-based Encryption
- Cloud DES Algorithm

A. Identity Based Encryption

Identity-based encryption (IBE) is one of the public key encryption. In this type of public-key encryption in which the public key of a user have some unique information about the identity of the user .For example user email address may be used as identity.This means that a sender who has access to the public parameters of the system can encrypt a message using e.g. the text-value of the receiver's name or email address as a key. The receiver obtains its decryption key from a central authority, which needs to be trusted as it generates secret keys for every user.

B. Attribute-based Encryption

Attribute-based encryption is is one of the public key encryption. In this type of method the secret key of a user and the ciphertext are dependent upon attributes. In such a system, the decryption of a ciphertext is possible only if the set of attributes of userkey and cipher text are matched. Attribute-based encryption (ABE) is a public-key based one-to-many encryption that allows users to encrypt and decrypt data based on user attributes. A promising application of ABE is flexible access control of encrypted data stored in the cloud, using access polices and ascribed attributes associated with private keys and cipher texts. One of the main efficiency drawbacks of the existing ABE schemes is that decryption involves expensive pairing operations and the number of such operations grows with the complexity of the access policy. An ABE system with outsourced decryption largely eliminates the decryption overhead for users.

Ciphertext-Policy ABE

In ciphertext-policy attribute-based encryption (CP-ABE) a user's private-key is associated with a set of attributes and a ciphertext specifies an access policy over a defined universe of attributes within the system. A user will be ale to decrypt a ciphertext, if and only if his attributes satisfy the policy of the respective ciphertext.

key-policy attribute-based encryption

The key idea of a Key-Policy Attribute-Based Encryption scheme (KP-ABE) is the sender encrypt the message only once. The policy assigned for users' keys that used to determine if these users can be allowed to decryptIn a key-policy attribute-based encryption (KP-ABE) system, ciphertexts are labeled by the sender with a set of attributes, while user's private key is issued by the trusted attribute authority captures an policy that specifies which type of ciphertexts the key can decrypt. KP-ABE schemes are suitable for structured organizations with rules about who may read particular documents. Typical applications of KP-ABE include secure forensic analysis.

C.Cloud DES Algorithm

This approach is applicable for securing data on both the server and the clients. DES cipher block chaining is constructed for security architecture to eliminate stealing of the data.

D. Homomorphic Encryption

This scheme is applied in the cloud environment to protect the data. This Homomorphic encryption scheme allows executing computations on the encrypted data. It is only of the advanced cryptographic technique. In the major drawback of homomorphic encryption is explained. It has a slow processing time -during -computation

E. Searchable encryption

Searchable encryption scheme is a cryptographic technique that allows search of specific information in an encrypted content. A searchable encryption scheme is applied at high level inoder to encrypt the content that is available in search index so that it can hidden from others except the party that provide the authorised tokens

F. Symmetric Searchable Encryption

It is suitable for the environment where the client that searches the data and also he is responsible for generates it. . A Single Writer/Single Reader (SWSR) is derived from cloud storage terminology. SSE has two major advantages they are efficiency and security. It also has disadvantages such as functionality and tradeoff efficiency.

G.Asymmetric Searchable Encryption (ASE)

This scheme is suitable for the environment where the client that searches the data is different from the one whogenerates it. This scenarios is referred as Many Writer/Single Reader (MWSR).

VI CONCLUSION

Cloud computing is an emerging trend in industry and it is mainly used in storage, computations, and accessibility. The strength of cloud computing is the ability to to overcome some security issues.Many algorithms used for securing data on cloud. Security algorithms used for encryption and decryption can be implemented to enhance security framework over the network. To proceed with security in cloud ,I am doing research in the area of data security and integrity in cloud.

References:

[1] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343–1354, Aug. 2013.

[2]RashmiNigoti, Manoj Jhuria and Dr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing" International Journal of Emerging Technologies in Computational and Applied Sciences,Vol. 4, pp.141-146, March-May 2013.

[3] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 6571, D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, Eds. Berlin, Germany: Springer-Verlag, 2011, pp. 53–70.

[4] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conf. Comput. Commun. Secur., 2007, pp. 456–465.

[5] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," in Proc. 20th USENIX Secur. Symp., 2011, p. 34.

[6] C. Gentry and S. Halevi, "Implementing Gentry's fully-homomorphic encryption scheme," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 6632, K. G. Paterson, Ed. Berlin, Germany: Springer-Verlag, 2011, pp. 129–148.

[7] Shi E, Bethencourt J, Chan T, Song D, Perrig A. Multi-dimensional range query over encrypted data. IEEE Symposium on Security and Privacy, IEEE Computer Society, Washington, DC, USA. 2007; 350–64.

[8]Baek J, Safavi-Naini R, Susilo W. On the integration of public key data encryption and public key encryption with keyword search. International Conference on Information Security (ISC '06), Lecture Notes in Computer Science. Springer. 2006; 4176.

[9]Baek J, Safavi-Naini R, Susilo W. Public key encryption with keyword search revisited. International conference on Computational Science and its Applications, Springer-Verlag. 2008; 1249–59.

[10] Fuhr T, Paillier P. Decryptable searchable encryption. International Conference on Provable Security, Lecture Notes in Computer Science, Springer, 2007;