Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 01, January-2018

Data Security in Cloud using AES

Smitha Nisha Mendonca
Department of Computer Science and Engineering
M.I.T.E, Moodbidri
Karnataka, India

Abstract- **Cloud computing is a future generation technology for IT enterprise. It has different characteristics like virtualization, multi-user, scalability and many more. It also provides on demand computational infrastructure which has the power to reduce the cost to build the IT based services. It can provide different types of service over the internet. One of the important services provided by the cloud is storage where users can keep their data as per the requirement. It is a challenging issue for the user as all the data are stored in some inter-connected resource pool but this resource pool is situated over different places of the world. An unauthorized user may be access this data through the virtual machines. So, it is the dark side of cloud data storage. This insecurity creates a big problem for users. Therefore data security in cloud computing is a major problem. Currently, AES is regarded as the most popular symmetric cryptographic algorithm. It is very significant to develop high performance AES to further broaden its widespread application.**

Keywords- Cloud Computing, Data Security, AES.

I. INTRODUCTION

Cloud refers to storing the user's data in a remote database instead of storing it in the hard disk of their own computer. Cloud delivers computing resources as a service in a scalable manner to the clients by means of Internet which eliminates the need of setting up company's own data center or server. These resources are offered on demand and customers pay for their level of usage.

National Institute of Standards and Technology (NIST) defines Cloud as "a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable resources that can be rapidly provisioned and released with minimal management effort or service provider interaction". There are five essential characteristics of cloud, three cloud service models and four cloud deployment models [1][2].

Five essential characteristics of cloud are [8]:

- Broad Network access: Resources available over the network are open to users by means of their phones, laptops and so on.
- Rapid Elasticity: Elasticity refers to scalability of resources according to the need of the user.
- Measured Service: The cloud provider monitors or measures and controls the services for various reasons like billing, resource optimization and planning.
- On-demand self-service: A user will cater the resources based on his requirement without interacting directly with every provider.
- Resource Pooling: Resources are shared to aid many customers based on multi-tenant model. The resources are allocated and reallocated in a dynamic manner according to user's necessity.

The various deployment models in cloud are as follows [8]:

- Public: The cloud infrastructure functions for common public and is possessed by an organization promoting cloud services. Services are available for general user over the internet.
- Private: The cloud infrastructure functions for a private business. It's like a virtualized datacenter operating within firewall.
- Community: The cloud infrastructure is made common to several organizations with the same principles and agreement consideration. It is possessed, administered, and controlled by a single or others of the organization in the community or a third party and it shall be on or off site.
- Hybrid: The cloud infrastructure is a grouping of clouds (public, private or community). The user may place less critical information in the public cloud while more critical data residing in the private cloud.

The delivery models in cloud are [8]:-

- Software-As-a-Service (SaaS): Client can access the software and the data associated with it on cloud through a browser. The user does not handle or administer the cloud infrastructure as well as network and servers.
- Platform-As-a-Service (PaaS): Client can utilize the provider's applications running on a cloud infrastructure and may be accessed from user devices with the help of interfaces like web browser.
- Infrastructure-As-a-Service (IaaS): Client can order resources based on their demand and they can set up and run any software as well as operating systems and applications. The user handles the resources like operating system, storage and applications.

One of the advantages of Cloud Computing is that data can be shared among various organizations. However, this advantage itself poses a risk to data. In order to avoid potential risk to the data, it is necessary to protect data repositories. Generally, data security deals with data protection. Security involves protecting the data from being lost, destroyed, corrupted, modified or disclosed. Instead of storing the data locally, users store them in cloud. So, correctness and availability of data must be assured. The primary concern in cloud computing is the protection of user data which is the major area of research.

II. DATA SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing implements three services such as SaaS, PaaS and IaaS to the end-user. In these service models different levels of security are provided in cloud computing environment. Efficient security technology in cloud computing is required to have a secured cloud computing and to speed up cloud element in SaaS service model such data security, data integrity, identity management, data location, data availability etc. are to be considered for better data security in cloud computing[7].

i) Data Security and Data Protection- Once the client hosts data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. Incorrect access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data.

ii) Data Integrity- By providing security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to explain what happened to a certain dataset and at what point. It may be necessary to have exact records as to what data was placed in a public cloud. When such data integrity requirements exist, the origin and custody of data or information must be maintained in order to prevent tampering or to prevent the exposure of data beyond the agreed territories.

iii) Data Location and Relocation- Cloud computing offers data mobility. Consumers are often not aware of the location of their data. When an enterprise has some sensitive data that is kept on a storage device in the cloud, they may want to know location where their data is stored safely. This requires an agreement between the cloud provider and the consumer that the data should stay in a particular location or reside on a given server. It is often moved from one place to another place in-order to secure the data in cloud. Cloud providers have contracts with each other which are called as SLA (Service Level Agreement) and they use each other’s resources.

iv)Data Availability- Customer data is normally stored in chunks on different servers which resides in different locations or on different clouds. In this case, data availability becomes a major issue as the availability of uninterruptible and seamless provision becomes relatively difficult. So it is important for the provider to provide proper data availability to the authorized user.

v) Identity Management- Each user uses his identity for accessing a cloud service. The provider should provide an identity management system for providing authentication and authorization. This is an important issue for both provider as well as the user in a cloud computing environment.

III. LITERATURE SURVEY

Encryption is a well-known technique for preserving the privacy of sensitive information. It is being adopted in many secure cloud computing applications. Different cryptographic techniques are used for encrypting the data these days. Cryptography has increased the level of data protection for assuring content integrity, authentication, and availability. Various Cryptographic techniques are [3]:-

1. Advanced Encryption Standard - AES is a symmetric key algorithm in which same key is used for both encryption and decryption of data. While AES is a widely-adopted encryption scheme for data on cloud storage, it limits many application functionalities such as search, logical operations and mathematical calculation.

2. Public Key Cryptography- Public key cryptography provides the foundation for both key management and digital signatures. In key management, public key cryptography is used to distribute the secret keys used in other cryptographic algorithms (e.g. AES). For digital signatures, public key cryptography is used to authenticate the origin and protect the integrity of data. Public-key cryptography demands considerable computing resources. The techniques under this scheme are Rivest-Shamir-Adleman (RSA) scheme and Elliptic Curve Cryptography (ECC).

3. Searchable Encryption- There are three techniques under this scheme. They are Searchable Symmetric Encryption (SSE), Public Key Encryption with Keyword Search and Deterministic Encryption. Symmetric searchable encryption (SSE) is appropriate in any setting where the party that searches the data is also the one who generates it. Public Key Encryption with keyword search scheme is appropriate in any setting where the party searching the data is different from the party that generates it. Deterministic encryption schemes are cryptographic systems which always produces the same cipher text for a given plain text and key even over separate executions of the encryption algorithm.

4. Order Preserving Encryption Scheme- This is a deterministic encryption algorithm. It produces cipher text that preserves the numerical ordering of plain text. The basic idea of this scheme is that it takes the input as a user-provided target distribution and transforms the plain text values in such a way that the transform preserves the order while the transformed values follow the target distribution.

5. Homomorphic Encryption- Homomorphic encryption allows us to encrypt the data in a way such that performing a mathematical operation on the encrypted data and decrypting the result produces the same answer as performing an analogous operation on the unencrypted data. The correspondence between operations performed on unencrypted data and the operations performed on encrypted data is known as a homomorphism. Some of the techniques under this scheme are Fully Homomorphic Encryption, Fully Homomorphic Encryption over the Integers and Homomorphic evaluation of AES.

6. Key Management- In order for encryption to work effectively, it is important to manage the encryption keys securely. Even if a cloud service provider provides encryption, they might access the keys. When encrypted data is stored in the cloud, the keys used for encryption

should be kept separate and should only be accessed by the end user. Key management involves the creation, use, distribution and destruction of encryption keys. Some of the techniques available under this scheme are Traditional Key Management, Stateless Key Management and Homomorphic Key Management System.

IV. ADVANCED ENCRYPTION STANDARD (AES)

AES stands for Advanced Encryption Standard. It is a symmetric encryption algorithm developed by two Belgian cryptographers Joan Daemen and Vincent Rijmen. It is an algorithm which performs encryption and decryption. The original information is known as plain text and the encrypted form is known as cipher text. The cipher text contains all the information of the plaintext but it is not in a format readable by a human or computer. The encrypting procedure varies depending on the key which changes the detailed operation of the algorithm. Without the key, the cipher text cannot be used to encrypt or decrypt [5].

AES Encryption

The AES algorithm operates on a 128-bit block of data and executed for Nr - 1 loop times. A loop is called as a round and the number of iterations in a loop, Nr can be 10, 12, or 14 which depends upon the key length. The key length can be 128, 192 or 256 bits in length respectively. The first and last round differ from other rounds because in that there is an additional Add Round Key transformation at the start of the 1st round and also Mix Column operation is not performed in the last round [9]. The various steps during encryption are given below:

1. Substitute Bytes Transformation
This stage (known as Sub Bytes) is simply a table lookup using a 16×16 matrix of byte values called an s-box. This matrix contains all possible combinations of an 8 bit sequence (28 = 16×16 = 256). The matrix that gets operated throughout the encryption is known as state. In this round each byte is mapped to a new byte in the following way: the leftmost nibble of the byte is used to specify a particular row of the s-box and the rightmost nibble specifies a column. For example, the byte {95} selects row 9 and column 5 which turns out to contain the value {2A}. This is then used to update the state matrix [4][10].

2. Shift Rows Transformation
In Shift Rows transformation, the rows of the state are shifted in cylindrical manner to the left. Any entries that fall off are re-inserted on the right side of row. Row 0 which is the 1st row is not shifted and remains as it is. Row 1 which is the 2nd row is shifted one byte to the left; row 2 which is the 3rd row is shifted two bytes to the left and row 3 which is last is shifted three bytes to the left. The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other [4][10].

3. Mix Columns Transformation
This stage is basically a substitution but it makes use of arithmetic of GF (2^8). Each column is operated individually where each byte of a column is mapped to a new value which is a function of all four bytes in the column. The transformation can be determined by the following matrix multiplication on state. Each element of the product matrix is the sum of product of elements of one row and one column. In this case the individual addition and multiplication are performed in GF (2^8) [4][10].

4. Add Round Key Transformation
In this stage, 128 bits of state are bitwise XORed with the 128 bits of the round key. This operation is viewed as a column wise operation between 4 bytes of a state column and one word of the round key. This transformation is simple which helps in efficiency but it also affects every bit of state [4][10].

AES Decryption
Decryption is the reverse process of encryption. Inverse round transformations are performed in decryption process to get original plain text. The round transformation of decryption uses the following functions [9][4]:

1. Add Round Key

2. Inverse Mix Columns

3. Inverse Shift Rows

4. Inverse Sub Bytes

1. Add Round Key

This operation is the inverse of encryption, since it only involves an application of the XOR operation.

2. Inverse Shift Rows Transformation
Inverse Shift Rows function is the same as Shift Rows, only in the opposite direction. The 1st row is not shifted, while the 2nd, 3rd and 4th rows are shifted right by one, two and three bytes respectively.

3. Inverse Sub Bytes transformation
The Inverse Sub Bytes transformation is done using an already calculated substitution table called Inverse S-box. That Inverse S-box table contains 256 numbers (from 0 to 255) and their corresponding values.

A. How AES works in cloud environment?

User's data can be made secure in the cloud using AES encryption [6].

- A user decides to use cloud services and transfer his data to the cloud.
- User then submits his service requirements to the Cloud Service Provider (CSP). She/he chooses the provider offering best services.
- When migration of data to the chosen CSP takes place and whenever an application uploads any data to the cloud, the data is encrypted and then sent. This encryption is done using AES algorithm.
- Any requests to read the data will happen after it is decrypted on the users end. Therefore plain text data can then be read by the requesting application.

The plain text data is never written anywhere on cloud. The key is never stored next to the encrypted data since it may compromise the key. To store the keys, a physical key management server is installed in the user's location. This encryption method protects the data and the encryption keys and guarantees that they remain under users control and are never exposed in storage or in transit.

V. CONCLUSION

Although cloud computing is the new emerging technology that presents a good number of benefits to the users, it faces lot of security challenges. In this paper various encryption techniques are discussed to overcome the risk involved in cloud computing. Among these, AES encryption is the fastest method which has flexibility and scalability and is easily implemented. AES algorithm has a high level of security because 128, 192 or 256-bit keys are used in this algorithm. It shows resistance against a variety of attacks such as square attack, key attack, key recovery attack and differential attack. Therefore, AES algorithm is a highly secure encryption algorithm. Data can also be protected against future attacks such as smash attacks. AES encryption algorithm has minimal storage space and high performance without any weakness and limitation while other symmetric algorithms have weaknesses and differences in performance and storage space.

ACKNOWLEDGMENT

I would like to acknowledge the support provided by the Department of Computer Science and Engineering at Mangalore Institute of Technology and Engineering (MITE), Moodbidri, Karnataka.

REFERENCES

[1] Ahmed Albugmi, Madini.O.Alassafi, Robert Walters, Gary Wills “Data Security in Cloud Computing”, Fifth International Conference on Future Generation Computation Technologies (FGCT), IEEE, 2016

[2] Farrukh Shahzad,”State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions”, The 6th International Symposium on Applications of Ad hoc and Sensor Networks, (AASNET’14)

[3] Chungsik Song, Younghee Park, Jerry Gao, Sri Kinnera Nanduri, William Zegers, “Favored Encryption Techniques for Cloud Storage”, 2015 IEEE First International Conference on Big Data Computing Service and Applications.

[4] Vishal R. Pancholi, Dr. Bhadresh P. Patel, “Enhancement of Cloud Computing Security with Secure Data Storage using AES”, IJIRST –International Journal for Innovative Research in Science & Technology, Volume 2 , Issue 09, February 2016

[5] Ali azougaghe, Zaid kartit, “An efficient algorithm for data security in cloud storage”, 2015 15th International Conference on Intelligent Systems Design and Applications (ISDA), IEEE

[6] Abha Sachdev, Mohit Bhansali, “Enhancing Cloud Computing Security using AES Algorithm”, International Journal of Computer Applications (0975 – 8887) Volume 67– No.9, April 2013

[7] M.Sugumaran, BalaMurugan,Kamalraj, “An Architecture for Data Security in Cloud Computing”, 2014 World Congress on Computing and Communication Technologies, IEEE

[8] Devi T, Ganesan R, “Data Security Frameworks in Cloud”, International Conference on Science, Engineering and Management Research (ICSEMR 2014), 2014 IEEE

[9] Pradnya Katkade1, Dr.G.M Phade, “Application of AES Algorithm for Data Security in Serial Communication”

[10] Poonam M. Pardeshi, Prof. Bharat Tidke, “Improving Data Integrity for Data Storage Security in Cloud Computing”, International Journal of Computer Science and Information Technologies, Vol. 5, 2014.