International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 10 | Oct 2018 www.irjet.net p-ISSN: 2395-0072

CLOUD DATA SECURITY USING AES ALGORITHM

Prof. S. Delfin[1], Rachana Sai. B[2], Meghana J.V[3], Kundana Lakshmi. Y[4], Sushmita Sharma[5]

[1]S.Delfin, Assistant Professor, Dept. of Computer Science and Engineering, SRM IST, Tamil Nadu, India
[2]Rachana Sai. B, Student, Dept. of Computer Science and Engineering, SRM IST, Tamil Nadu, India
[3]Meghana J.V, Student, Dept. of Computer Science and Engineering, SRM IST, Tamil Nadu, India
[4]Kundana Lakshmi. Y, Student, Dept. of Computer Science and Engineering, SRM IST, Tamil Nadu, India
[5]Sushmita Sharma, Student, Dept. of Computer Science and Engineering, SRM IST, Tamil Nadu, India

---

Abstract:- *Popular security experts decrypt the most demanding feature of cloud computing security. Cloud computing allows both large and small companies to have the opportunity to use Internet-based services .so that they can lower the start-up costs, capital expenditures, access applications only if there is a need, use services on pay-as-you-use basis, and quickly lower or increase ability. As the authors offer the years of unparalled skill and knowledge, they discuss all the highly challenging topics like data ownership, privacy protections, data mobility, standard of service and service levels, bandwidth costs, data protection, and support. Advanced Encryption Standard is one on the most regular and mostly symmetric block cipher algorithm. This algorithm has a specific form to encrypt and decrypt subtle data and is put in all hardware and software. It is highly tough to hackers to get the actual data when encrypting by AES. Till date there is no proof to crack this algorithm. AES has the capacity to deal with 3 dissimilar key sizes such as AES 128, 192 and 256 bit. Each of its code has 128 bit.*

***Key Words*: AES Algorithm, Cloud Computing, Data Security, Encryption, Decryption**

1. INTRODUCTION

Internet communication is playing the important role to transfer large amount of data in various fields. Some of data might be transmitted through insecure channel from sender to receiver. Various methods and techniques are being used by public and private sectors to secure sensitive data. This is done to secure data from invaders because of the security of electronic data is a critical issue. Cryptography is one of the most notable and desired techniques to protect the data from attackers by using two essential processes. These processes are listed as Encryption and Decryption. Encryption is the process of converting the data to stop it from attackers to read the original data clearly. Encryption involves conversion of plain text to unreadable format. It is known as cipher text. The user cannot read the above format. Hence, the next process that is carried out by the user is Decryption. Cloud computing is a promising and emerging technology for the next generation of IT applications. The hurdles towards the fast growth of cloud computing are privacy issues and data security. Cryptography is one of the most important and prominent skill to secure the data from hackers by using two processes that is Encryption and Decryption. AES encryption is the speedy method that has the flexibility and is easy to implement. Whereas, the required memory for AES is less than the Blowfish algorithm. It shows resistance against a different variety of attacks such as key attack, key recovery attack, square attack, and differential attack. Therefore, AES is a highly secure encryption. Data can also be protected against future attacks like smash attacks. AES encryption has minimum storage space and high implementation without any limitations and weaknesses while other symmetric algo have some differences in performance and storage space and weaknesses.

2. EXISTING SYSTEM

In the existing system, there exist security issues for storing the data in cloud. Cloud computing security includes various problems like information loss, accessibility of cloud, multi tenancy, internal threats, leakage, identity management, etc. It is not easy to implement the security measures that satisfies the security needs of all the users. It is because users may have divergent security concerns depending upon their purpose of using the cloud services. Cloud service provider has bestowed an excellent security layer for the user and customer. The user needs to ensure that there is no loss of data or misuse of data for other users who are using the same cloud. The cloud service providers should be capable of surviving against cyber-attacks. Not all the cloud providers have the capability of securing data. Various algorithms are being implemented to eradicate the security issues in cloud storage of data.

3. ARCHITECTURE

Advanced Encryption Standard technique performs in accordance to both hardware and software platforms under a broad spectrum of environments. It includes 64-bit and 8-bit platforms. Its inherent parallelism eases efficient use of processor resources resulting in very good software performance. The algorithm has many advantages like less memory allocation for implementation, suitable for restricted-space environments. The structure of algorithm has good scope for profiting from instruction-level parallelism. There are no weak keys in AES. The algorithm supports any key sizes and block sizes that are greater than 128 bits. Statistical analysis of the cipher text has not been possible even after using huge number of test cases. No differential and linear cryptanalysis attacks have been yet proved on AES.

Fig No.1.1 Cloud Data Security System Architecture

4. PROPOSED SYSTEM

Cryptography is one of the most notable and desired techniques to protect the data from attackers by using two essential processes. These processes are listed as Encryption and Decryption. Encryption is the process of converting the data to stop it from attackers to read the original data clearly. Encryption involves conversion of plain text to unreadable format. It is known as cipher text. The user cannot read the above format. Hence, the next process that is carried out by the user is Decryption. In the world of computing, there exist security issues for storing the data in cloud. In order to secure data in cloud AES encryption technique is used in this project. Advanced Encryption Standard is a block cipher with a block length of 128 bits. It permits three different key lengths: 256, 192,128 or bits.

5. IMPLEMENTATION OF AES ALGORITHM

The matrix of 4x4 consisting of 128 bytes input block is known as the state array. The process of encryption revolves around four stages namely mix, columns, sub bytes, add round key and shift rows.

• Sub Bytes – It is defined as substitution step. It is non-linear. Each byte is restored with another according to S-box. The operation gives an indirect proportion in cipher. The resultant matrix consists of four columns and four rows.

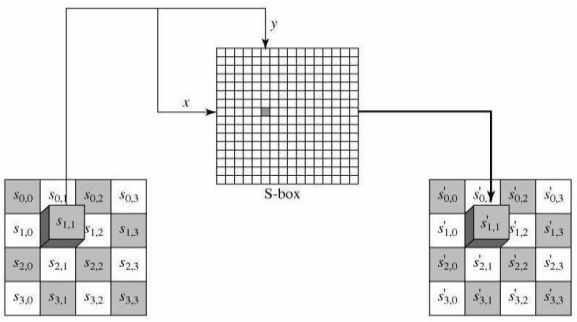

Fig No. 1.2 Byte substitution

• Shift Rows – It is stage where each row is rotated repetitively a definite number of times. It is also known as permutation. The four rows in the matrix are rotated accordingly. The rows are shifted to the left. Shift is carried out as Row1 is not rotated. Row2 is shifted one byte place to the left. Row3 is shifted two places to the left. Row4 is shifted three places to the left. The resultant matrix consists of the 16 bytes but rotated with respect to each other.

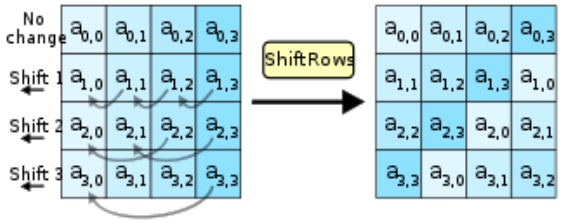

Fig No. 1.3 Shift Rows

• Mix Columns –In this step, each column is changed using matrix multiplication. Each column consists of four bytes. The resultant matrix consists of 16 bytes. The input is taken for each column. It takes four bytes. The output produces four bytes which is entirely different from the four bytes given as input

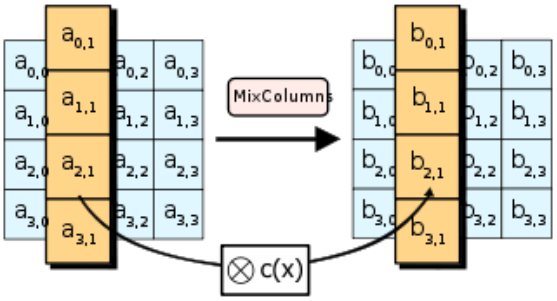

Fig No.1.4 Mix Columns

• Add Round Key – The round key is bounded to each byte of state. In this particular step, the matrix is XO-Red with the round key. A 4x4 matrix represents the original key. It contains 128bits. This 4 words key where each word is of 4 bytes, is converted to a 43 words key. The first four words represent W[0], W[1], W[2], and W[3].

6. MODULE IMPLEMENTATION

The proposed system is designed to maintain security of not only text files but also image files of any format (.jpg, .jpeg, .png). This proposed system uses Advances Encryption Standard algorithm to perform encryption. When user uploads the image or text files in Cloud Storage, the file is encryptrd. Inverse AES algorithm is used decrypt the file when the user downloads it from Cloud Storage. This increases the security. The system is designed to maintain security of text files and image files. The proposed system design focuses on the following objectives which are helpful in increasing the security of data storage. The modules are classified into partially independent and partially dependent modules such as the data owners module, data user module, cloud administrator module.

1. DATA OWNER MODULE

In this module, data owner has legitimate rights and complete control over a single piece of data or collection of

data elements of the cloud. In this module, data owner has the authority to edit, modify, create, share and restrict access to the cloud data. Data owner is the one who wants to spread his business with the help of website then he/she has to set up the servers and maintenance of servers which leads to the high cost. In this system, the owner of data can access and archive the data stored by the Cloud Service Provider. The data user has to be given authority by data owner to access, manipulate or perform any action on cloud data. The following are features of data owner module.

- Data user sends a key request to data owner and intern to the cloud.
- File upload section is where the user uploads files either of .txt, .jpg, and .png format. The file then is encrypted using the key generated by AES algorithm in the cloud administrator module.
- Encryption section of this module encrypts text files and also image files of any format (.jpg, .jpeg, .png). This module uses AES algorithm to generate encryption.
- When user uploads the image or text files in Cloud Storage, the file is encryptrd. Inverse AES algorithm is used decrypt the file when the user downloads it from Cloud Storage. This increases the security.
- View user request section of this module is merely a page to view key requests sent by the data user along with additional information.

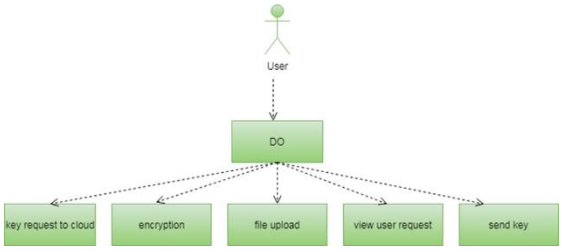

Fig No. 1.5 Use Case Diagram of Data Owner

2. DATA USER MODULE

Data user uses the cloud to store data and access it at any point of time. The data user just wants to use the application software such as Ms Office, Paint Brush, and Image Processing Software etc. This sort of service is provided by Software as a Service model of cloud computing which gives freedom to the user from getting license of software. The features of data user module include the following;

- Registration module is present for new users to register by providing details such as username and password.
- Log-in module allows user to log in to one's cloud data segment.
- The user can search for required files present in the cloud storage. These files are uploaded by the data owner. They are present in encrypted format. Hence, data user must request data owner for key to decrypt the file and download it.
- The request for key can be sent in the key request page of this module.
- Using the key sent by data owner, the data user can decrypt the file and download it.

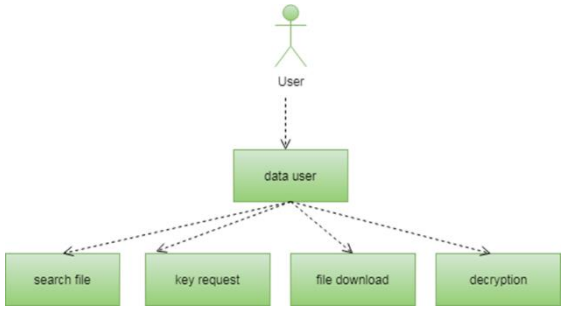

Fig No. 1.6 Use Case Diagram of Data User

3. CLOUD ADMINISTRATOR MODULE

The cloud administrator module depicts the cloud service providers in the system. There are various cloud service providers which includes Microsoft azure, cisco, Google, Verizon, etc. In this module, cloud administrators have two main responsibilities ie., it configures the Cloud Management service and it supervises and manages the services. The features of cloud administrator module include the following:

- The cloud administrators can outlook pending requests for cloud resources
- It accepts to change requests linked with moderations to cloud resource.
- It can view and examine the data on cloud resource deployments
- It supervises key metrics and requests for cloud resources
- It helps to run Discovery on the cloud resources

7. CONCLUSIONS

Cloud computing is a promising and emerging technology for the next generation of IT applications. Cryptography is one of the most important and prominent skill to secure the data from hackers by using the essential processes that is Encryption and Decryption. AES encryption is the speedy method that has the flexibility and is easy to implement.

Data can also protect against future attacks such as smash attacks. AES encryption algorithm has high performance and very little storage space without any restrictions while other

symmetric algorithms have some restrictions and differences in storage space and performance. The implementation of Advanced Encryption Standard for securing data bestows benefits of less computation time and less memory consumption in contrast to other algorithms. Though each cloud infrastructure has its own security strengths; the user can choose infrastructure according to his security. Each of the cloud providers has their own set of rules, pricing, flexibility, support and other important parameters. The key consideration dealt in this proposed system is the encryption technique to secure data for the users. The approach used in this work, will help to make a strong structure for security of data in cloud computing field or web.

8. FUTURE ENHANCEMENT

Security is an important aspect of cloud computing. The strength of cloud computing is the ability to manage risks in particular to security issues. Security algorithms can be used for implementing encryption and decryption techniques to secure data .In future, the key length can be expanded using any other key generation algorithm. The AES algorithm uses 128 bits. This includes ten rounds or cycles of AES algorithm. In future this can be extended to 192 or 256 bits. If 192 bit key is used, the number of cycles will be 12. When the key size is 256 bits there are 14 rounds. The increased key size can produce more number of keys and also the security can be enhanced. The storage node availability is checked by the server. In cloud, there are several storage nodes available. In this present work, at the maximum of four nodes are taken into consideration. In future, this value can be extended. In the present work, there is a need for storing the values of IP address and the random keys. This is time consuming and it may take some amount of memory space. In future, using some other techniques, the time and memory space can be minimized. Cost of the storage node can be calculated and reduced. In this work the storage nodes are selected from the same cloud. In future select the storage nodes can be selected from different cloud providers and the cost calculated. And using this, it can be decided to reduce the cost. The cost calculated by different cloud providers may vary. Depending on the time whether it is peak time or not, the cost will be calculated by CSPs. The future work of the proposed system will be extended by improving speed of the decryption process and also planned to reduce the size of the cover image using the compression technique.

REFERENCES

[1] Ch. Chakradhara Rao and A.V.Ramana,"Data Security in Cloud Computing", International Journal of Current Trends in Engineering and Research

[2] Arijit Ukil, Debasish Jana and Ajanta De Sarkar, "A Security Framework In Cloud Computing Infrastructure", International Journal of Network Security and Its Applications, Vol.5, Issue No.5

[3] Nasarul Islam.K.V,"Analysis of Various Encryption Algorithms in Cloud Computing", International Journal of Computer Science and Mobile Computing, July 2017

[4] Rachna Arora and Anshu Parashar, "Secure user data in cloud computing using encryption algorithms",International Journal of Engineering Research and Applications , July-August, 2013

[5] Amrita Parashar, "Services & Security of Cloud Computing Using DES",International Journal of Computer & Mathematical Sciences, May 2016

[6] Roshani Raghatate , Sneha Humne and Roshna Wadhwe, "A Survey on Secure Cloud Computing using AES Algorithm",International Journal of Computer Science and Mobile Computing, December 2014

[7] V.Surya, S.Ranichandra and R.Ranjani, "Secure Cloud Storage Using AES Encryption", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 6, Issue 6,ISSN 2320-9801