International Journal of Scientific Research in Science, Engineering and Technology

Print ISSN - 2395-1990
Online ISSN : 2394-4099

OPEN ACCESS

Available Online at :www.ijsrset.com
doi : https://doi.org/10.32628/IJSRSET25122213

Secure File Storage System Using Cloud

Sudhanshu M. Wasu[1], Dr. Sudhir W. Mohod[2]

[1]Student, Department of Computer Science and Engineering, BDCE, Sewagram, Wardha, Maharashtra, India

[2]Professor and Head, Department of Computer Science and Engineering, BDCE, Sewagram, Wardha, Maharashtra, India

ARTICLEINFO

Article History:

Accepted : 01 May 2025
Published: 04 May 2025

Publication Issue :
Volume 12, Issue 3
May-June-2025

Page Number :
25-29

ABSTRACT

Cloud computing basically comes to focus on IT, a way to increase capacity or add potentiality on the fly without investing in new infrastructure, training new personnel, or licensing new software. It encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends its existing capabilities. It is often provided "as a service" over the Internet, typically in the form of infrastructure as a service (IaaS), platform as a service (PaaS), or software as a service (SaaS). Microsoft Azure and Google App Engine are the examples of platform as a service. The fast growth in field of "cloud computing" also increases rigorous security concerns. In today's world most of the communication is done using electronic media. Data Security is widely used to ensure security in communication, data storage and transmission. We have Advanced Encryption Standard (AES) which is accepted as a symmetric cryptography standard for transferring block of data securely. The available AES algorithm is used for text data and it is also suitable for image encryption and decryption to protect the confidential image data from an unauthorized access. This project proposes a method in which the image data is an input to AES Encryption to obtain the encrypted image, and the encrypted image is the input to AES Decryption to get the original image.

Index terms: Cloud Computing, Security, Encryption, Decryption, AES, DES.

INTRODUCTION

Nowadays cloud computing is used in many areas like industry, military colleges etc. to storing huge amount of data. We can retrieve data from the cloud on the request of the user. To store data on the cloud we have to face many issues. There are multiple ways to provide the solution to these issues. Cryptography and steganography techniques are more popular nowadays for data security. Use of a single algorithm is not effective for high level security of data in cloud

computing. In this project we have introduced a new security mechanism using a symmetric key cryptography algorithm and steganography.

File security concerns arise because both user's application and program are residing in the provider premises. The cloud provider can solve this problem by encrypting the files by using encryption algorithm. This project presents a file security model to provide an efficient solution for the basic problem of security in local system environment. In this model, hybrid encryption is used where files are encrypted by three algorithms coupled with file splitting which is used for the secured communication between users and the servers.

Encryption is one of the principal means to guarantee the security of sensitive information. It is great for everything from sending sensitive information to securing your email, keeping your cloud storage safe, and even hiding your entire operating system. Many encryption algorithms are widely available and used for information security. Encryption algorithms are classified into two groups: Symmetric-Key and asymmetric-Key encryption.

Symmetric key encryption is a form of cryptosystem in which encryption and decryption are performed using the same key. It is also known as conventional encryption. Asymmetric key encryption is a form of cryptosystem in which encryption and decryption are performed using different keys i.e. public key and private key. It is also known as public key encryption. Asymmetric encryption techniques are about 1000 times slower than symmetric encryption which makes it impractical when trying to encrypt large amounts of data. Also to get the same security strength as symmetric, asymmetric must use a stronger key than symmetric encryption technique.

LITERATURE REVIEW

In [1], the authors presented a new algorithm which does two works: lossless compression and encryption of binary and gray-scale pictures. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology.

The authors of [2] proposed an algorithm based on hash function. Firstly it does pre-processing operation to shuffle one half of image, then a hash function to generate a random number mask. The mask is then XOR with the other part of the image which is going to be encrypted.

In [3], Cloud Computing is one of the revolution in Information Technology (IT) that can share resources, services and data through a network among users. As users have same rights on the network to transfer data, data is vulnerable to be attacked by an unauthorized person. Lately, data security in a system only concentrates on data storage on cloud by utilizing internet security, but a little concentration is found during data transfer. By considering security as a serious problem, an encryption-based proposed system is presented to secure during data transfer. The authors thus proposed an approach to boost system security during data transfer in order to prevent data theft by unauthorized person. To prevent an attack by unauthorized person, Advanced Encryption Standard (AES) will be proposed to secure data transfer and storage in cloud computing.

Abdul. Elminaam et al. [4] studied about the performance of symmetric encryption algorithms. This paper provides evaluation of six of the most common encryption algorithms: AES, DES, 3DES, RC2, Blowfish and RC6. A comparison had conducted at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. Experimental simulation shows experimental results.

In [5], the performance of different security algorithms on a cloud network and on a single processor for different input sizes was studied. This paper aimed to find in quantitative terms like speed up ratio that benefits of using cloud resources for implementing security algorithms (RSA, MD5 and

AES) which is used by businesses to encrypt large volume of data.

Alanazi et al.[6] has done the comparative analysis of three encryption algorithms(DES, 3DES and AES) within nine factors such as key length, cipher type, block size, security, possible keys at 50 billion keys per second etc. study shows that AES is better than DES and 3DES.

OBJECTIVES

The objectives of the proposed system can be summarized as follows:

- To develop a secure file storage system that use public key cryptography to facilitate authorization of user for each file.
- The need of more light and secure encryption system for file information preserving system on the cloud.
- The file splitting and merging make the model infeasible to get attacked.

PROPOSED SYSTEM

In this proposed system AES, DES, RC2 algorithms are used to provide block wise security to data. LSB steganography technique is introduced for key information security. Key information contains which part of file is encrypted using by which algorithm and key. File is fragmented into 3 parts. Each and every part of file is encrypted using different algorithm. All parts of file are encrypted simultaneously with the help of multithreading technique. Data encryption Keys are inserted into cover image using LSB technique. Stego-Image is sent to valid receiver using email. For file decryption purpose reverse process of encryption is applied.

Proposed Cloud Computing Security Architecture:

In order to ensure file security on cloud, the above hybrid cryptosystem is deployed on cloud. We assume cloud server as trusted but in order to prevent tampering/misuse of data by intruder or data leakage or other security concerns, the data is stored at server in the encrypted form. We broadly classify the scheme deployed on cloud in three phases:

- Registration Phase
- Uploading Phase
- Downloading Phase

We used Azure toolkit to set up cloud environment.

A. Registration Phase:

In the Registration Phase, the client registers himself in order to upload and view his files to/from the cloud server.

B. Uploading Phase:

The files are uploaded by the client to the registered server. The encryption of uploaded files is done using the hybrid cryptosystem. The private keys are sent to user so that only the authenticated user is able to view his uploaded file.

C. Downloading Phase:

On successful authentication, the client will input the private key for the corresponding n slices. The private keys will decrypt the corresponding encrypted image. The decrypted files are merged to generate original file. The decrypted file is downloaded and viewed at client end.

Hybrid Cryptosystem Scheme:

In order to ensure file security on cloud, hybrid cryptosystem is being used. We assume that the remote server is trusted, so files are encrypted by server and finally encrypted files are stored at the server end. The hybrid cryptosystem uses a combination of:

- AES (Advance Encryption Standard)
- DES (Data Encryption Standard)
- RC2 (Rivest Cipher 2)

In a hybrid scheme, the performance of symmetric algorithm is integrated with security of asymmetric algorithm. The symmetric algorithm used in hybrid cryptosystem has best practice to avoid data misuse when compared with other symmetric algorithms. Also, in terms of throughput, Blowfish has best performance.

In hybrid cryptosystem, firstly, files uploaded files are sliced and each slice is encrypted by the corresponding key. Hybrid cryptosystem used to maintain security of the files has two phases:

- Encryption Phase
- Decryption Phase

A. Encryption Phase:

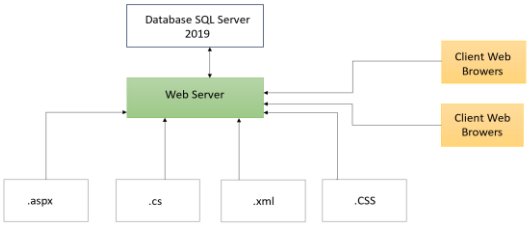
On the specification of user, the file being encrypted will be sliced into 'n' slices.

B. Decryption Phase:

At the decryption end, the user will provide the private keys, according to the number of slices (n) created during the encryption phase. Using the corresponding decrypted, file slices stored at server are decrypted. The decrypted slices will be merged to generate original file.

The various benefits are as summarized:

- The public key cryptography used helps to facilitate authorization of user for each file.
- The need of more light and secure encryption system for file information preserving system on cloud is satisfied.
- The file splitting and merging makes the model unfeasible to get attacked.



SYSTEM REQUIREMENTS:

- **Hardware Requirements:**
  - Processor –Core i3
  - Hard Disk – 160 GB
  - Memory – 4GB RAM or higher
  - Monitor
  - Active Internet Connection
- **Software Requirements:**
  - Windows 10 or higher
  - ASP.NET with C#
  - MS Visual Studio 2022
  - SQL Server 2019
  - XML, CSS
  - MS Azure

CONCLUSION

Data security and privacy of cloud data stored in Cloud Computing has full of challenges and many research problems are yet to be come which increases the security problem. The cloud data storage presented here through hybrid security algorithms using the symmetric key. The only difficult task is here that the key is secure. That are only accessible by the authorize user. And the purpose of using that key the is save the more time to store the large amount of data in cloud data storage. The purpose of these algorithm is generally in cloud data storage (server storage system) not in travelling the data between the user by secure channel.

REFERENCES

[1]. William Stallings, "Advance Encryption Standard," in Cryptography and Network Security, 4th Ed., India : PEARSON , pp. 134–165.

[2]. Atul Kahate, "Computer-based symmetric key cryptographic algorithm", in Cryptography and Network Security, 3th Ed. New Delhi : McGraw-Hill, pp. 130-141.

[3]. Manoj .B,Manjula N Harihar (2012, June). "Image Encryption and Decryption using AES", International Journal of Engineering and Advance Technology (IJEAT) volume-1, issue-5, pp.290-294.

[4]. Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M. (2008). Performance evaluation of symmetric encryption algorithms.

IJCSNS International Journal of Computer Science and Network Security, 8(12), 280-286.

[5]. Arora, P., Singh, A., & Tyagi, H. (2012). Evaluation and comparison of security issues on cloud computing environment. World of Computer Science and Information Technology Journal (WCSIT), 2(5), 179-183.

[6]. Alanazi, H., Zaidan, B. B., Zaidan, A. A., Jalab, H. A., Shabbir, M., & Al-Nabhani, Y. (2010). New comparative study between DES, 3DES and AES within nine factors. arXiv preprint arXiv:1003.4085.

[7]. Mandal, A. K., Parakash, C., & Tiwari, A. (2012, March). Performance evaluation of cryptographic algorithms: DES and AES. In 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science (pp. 1-5). IEEE.

[8]. Kakkar, A., Singh, M. L., & Bansal, P. K. (2012). Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication. In in Multinode Network", International Journal of Engineering and Technology Volume.

[9]. Sutton, E. Latency, Packet Loss and Encryption using DES with a VPN.

[10]. S. Pavithra, E. Ramadevi,(2012), Performance Evaluation of Symmetric Algorithmns.