Data Security Algorithm for Cloud

[1]U. ANUDEEP, [2]G. DIVYA, [3]L. SHALINI PRIYA,[3]D. BHARGAV
[1]UG Student, [2]UG Student,[3]UG Student, [3]UG Student
[1]Computer Science & Engineering,
[1]Dhanekula Institute of Engineering and Technology, Ganguru, India

Abstract: Now-a-days, cloud computing has become most popular paradigm both for service providers and customers over internet. Hence, these Cloud service providers are needed to ensure trust and security for users because the users are sharing their sensitive information on cloud which is very vulnerable. Cloud computing allows users to store their data remotely in cloud servers and these cloud servers are responsible for providing services according to their demand. When adopting data into the cloud the data security measures are identified by security challenges and how to handle these challenges. From the customer point of view data security and privacy are most the most important critical factors to be considered.

To enhance security in cloud computing, it is important to provide goals like authentication, authorization, and access control for data stored in the cloud. The three important goals of security system are Confidentiality, Integrity and Availability. Data encryption has been widely applied in many data processing areas. Various encryption algorithms have been developed for processing text documents, images, video, etc. If we are able to collaborate the advantages of the different existing encryption methods, then a new hybrid encryption method can be developed which offers better security and protection.

I. INTRODUCTION

The cloud is popular to store data and files due to the low costs, less maintenance and ease of access from any location. Apart from the private and public organizations, government services are looking for cloud based storage and services for their confidential data storage. Every cloud provider like Microsoft Azure, IBM, Amazon Web Services (AWS) and many others have provided their own technique to encrypt and decrypt the data. The cloud computing is widely used in private and public services organizations for storing huge amount of data which can be made available from any location. The usage of cloud is found in industry, military colleges, and private organizations. The data stored on the cloud is accessible by user authentication but for confidential access multiple layer of security is implemented. The algorithm of this multiple layer security is dependent on the level of privacy. To provide the solution to different levels of security, cryptography and steganography techniques are popular. Multiple algorithms must be incorporated to enhance the level of security in data storage. New technique, using symmetric key cryptography algorithm and steganography is proposed in this work.

While accessing the data on cloud front end interface, business layer and data storage layers are used. Though the front end resides on user computer, but the business and data layers reside on service provider premises. Hence the encryption algorithm is implemented by the cloud service provider. The challenge in encryption is that more complex logic slows down the reading and writing of the files on the server and hence the algorithm is applied only when it is needed. Encryption algorithm helps to solve this problem by encrypting the files. This purpose of this research is to present a file security model for the solution of security issue in cloud environment. In this model, hybrid encryption is used where files are encrypted by 6 algorithms coupled with file splitting which is used for the secured communication between users and the servers.

II. EXISTING SYSTEM

In this technique existence of data is not visible to all people. Only valid receiver knows about the data existence. Image steganography technique is used to produce high security for data. Secret data of user hide into image file. After adding text into image file, it looks like normal image file. DES algorithm is used for text encode and decode. Advantage of image steganography technique is providing security to text. Three-bit LSB technique used for image steganography. We can hide huge amount of into image using LSB steganography technique. AES is symmetric key cryptography algorithm. It supports three types of keys. For 128-bit key require 10 rounds, 192-bit key require 12 rounds and 256 bit key require 14 rounds [6]. In improved AES algorithm encryption and decryption time is reduced. Advantage of modified AES algorithm is providing better performance in terms of delay [1]. DES applies a single key for texts encode and decode. Size of key is 128 bits. In this algorithm many steps are executed randomly so illegitimate user cannot even guess the steps of algorithm. Provide high throughput is one of the advantages of symmetric key cryptography algorithms. [4] Improved DES algorithm uses 112-bit key size for data encode and decode. Key generation process is done using random key generation technique. It provides security to data. Disadvantage of this algorithm is essential maximum time for converting data into cipher text because it operates on single byte at a time.

Disadvantages of existing system:

Due to openness and multi-tenant characteristics of the cloud, the traditional security mechanisms are no longer suitable for applications and data in cloud. Some of the issues are as following:

- Due to dynamic scalability, service and location transparency features of cloud computing model, all kinds of application and data of the cloud platform have no fixed infrastructure and security boundaries. In the event of security breach, it is difficult to isolate a particular resource that has a threat or has been compromised.
- According to service delivery models of Cloud computing, resources and cloud services may be owned by multiple providers. As there is a conflict of interest, it is difficult to deploy a unified security measure.
- Due to the openness of cloud and sharing virtualized resources by multitenant, user data may be accessed by other unauthorized users.

III. PROPOSED SYSTEM

The Cryptographic data Encryption is one of the solutions to secure data in cloud computing platform. There are symmetric (e.g. DES, AES) asymmetric (e.g. RSA, EIGamal, ECC), Digital signature (MD5, SHA) algorithms are present and the combination of these algorithms form hybrid data security cryptographic algorithm.

Here proposing a combination of ECDSA, SHA256 and AES is used for sending and
receiving data message on the cloud.

The message file upload hybrid data security algorithm:

- The cloud user is having the data message or file to be secure before that has to be sent to the Cloud Service Provider.
- The ECDSA with SHA 256 message digest and corresponding digital signatures are generated in the client machine.
- The data message or file with public key is encrypted using AES encryption algorithm.
- The encrypted data or file is sent to cloud service provider.
- The data message file is then store it in to corresponding cloud server.

The message download hybrid data security algorithm:

- The cloud user has to request the cloud service provider to download his/her stored secure data message or file.
- The Cloud Server will check the hash value of the requested message or file.
- If the hash values have been matched, then the cloud server will perform the AES data or file decryption algorithm with private key of the requested cloud user.
- The Decrypted message or file is sent to corresponding requested cloud user.
- Now the decrypted original message or file is obtained.

IV. IMPLEMENTATION AND WORKING

This application consists of the following modules:

User-Registration Module

If any new user who wants to use the services 0f the cloud, they need to get registered with their details.

Cloud Module

In cloud module we will have two sub-modules

- User Module

  The user module will have request details to get access for cloud usage. The admin will have chance to activate and de-activate the services of user.
- Request Queue Module

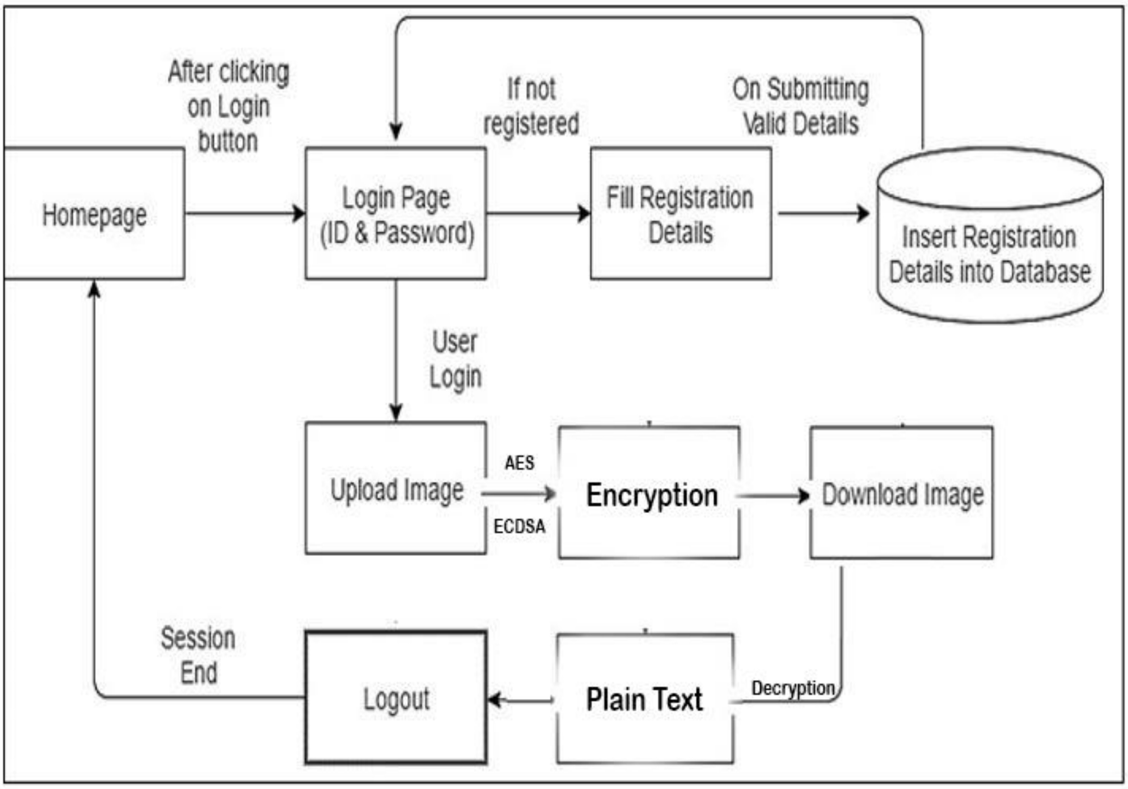
  Whenever user wants the data present in the cloud he will download it. All the download details of users will be present in the Request queue.

User Module

In User module we will have three sub-modules

- Upload Module

  In this module user can upload the sensitive data into cloud which will be secured. While uploading the plain text is converted into cipher text.
- Download Module: - In this module user will download the data from cloud. While downloading the cipher text is converted into plain text.
- Search Module: - In this module users can search for the data which is uploaded into cloud.


After clicking on Login button
If not registered
On Submitting Valid Details
Homepage
Login Page (ID & Password)
Fill Registration Details
Insert Registration Details into Database
User Login
Upload Image
AES
ECDSA
Encryption
Download Image
Session End
Logout
Plain Text
Decryption

ALGORITHMS

AES Algorithm:

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

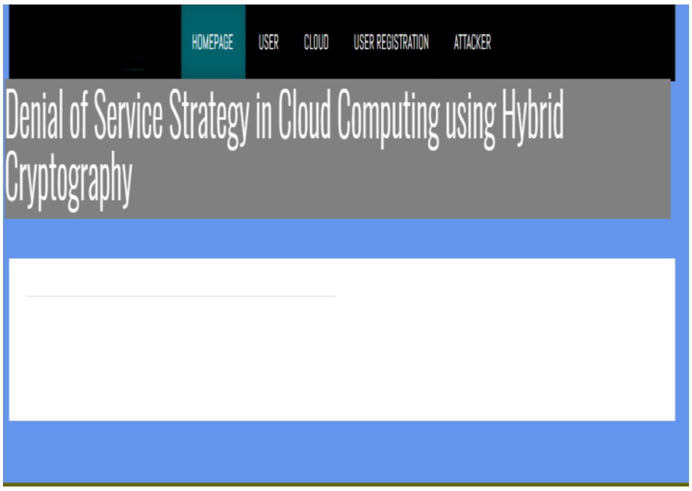
Elliptic Curve Digital Signature Algorithm:

Elliptic-curve cryptography (**ECC**) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-EC cryptography to provide equivalent security.

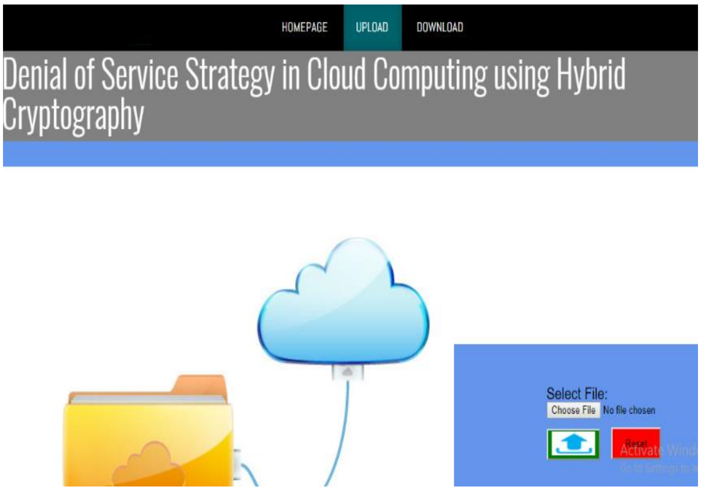
Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme

V. EXPERIMENTAL RESULT

After implementing and executing the system we get the following results. Below figure is the description for the cloud login page. We used java programming language and html along with operating system.

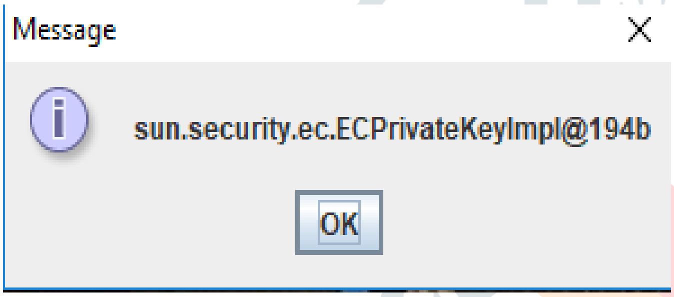


Denial of Service Strategy in Cloud Computing using Hybrid Cryptography

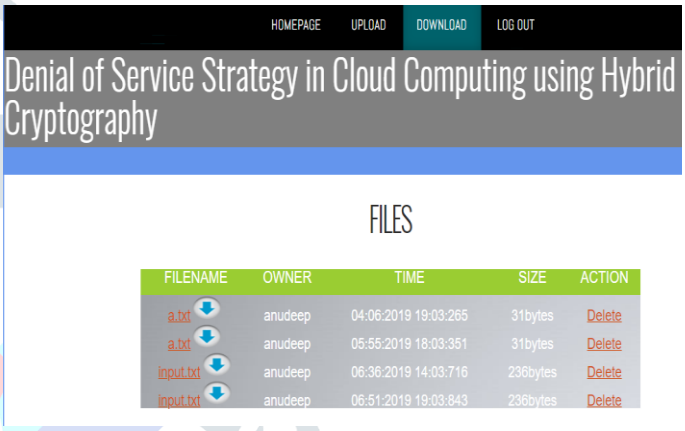


Denial of Service Strategy in Cloud Computing using Hybrid Cryptography

Select File: No file chosen



sun.security.ec.ECPrivateKeyImpl@194b



Denial of Service Strategy in Cloud Computing using Hybrid Cryptography

FILES

FILENAME	OWNER	TIME	SIZE	ACTION
a.txt	anudeep	04:06:2019 19:03:265	31bytes	Delete
a.txt	anudeep	05:55:2019 18:03:351	31bytes	Delete
input.txt	anudeep	06:36:2019 14:03:716	236bytes	Delete
input.txt	anudeep	06:51:2019 19:03:843	236bytes	Delete

VI. Conclusion

Data Security and Privacy of data stored in have full of challenges. Continuous research is going on to improve the data storage security. This paper presents hybrid security algorithms using the symmetric key. This approach helps in reducing the encode and

decode time and hence help in improving the performance for storing large data files in highly secured environment. Because the key is secured, it can only be accessed by the authorized user. The algorithm is built and computed on cloud server so that data

movement traffic is minimized. The solution proposed in this research provides additional layer of security by combining AES, DES, RC6, ECB, CBC, Triple DES algorithms to asymmetric cryptography. This technique helps to apply the key information on data storage (server storage system).

VII. References

1. Y Manjula, K B Shivakumar. Enhanced Secure Image Steganography using Double Encryption Algorithms, at International Conference on Computing for Sustainable Global Development IEEE, 2016.
2. Aarti Singh, Manisha Malhotra. Hybrid Two-Tier Framework for Improved Security in Cloud Environment, at International Conference on Computing for Sustainable Global Development IEEE, 2016.