JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

DATA FILE SECURITY ON CLOUD USING MULTIPLE ENCRYPTION

R. AIESHA SIDDIQUA[1] & G. RAMANJINAMMA[2]

[1]*PG Scholar, Department of CSE, B.I.T Institute of Technology, Hindupur, Andhra Pradesh, India.*

[2]*Assistant Professor, Department of CSE, B.I.T Institute of Technology, Hindupur, Andhra Pradesh, India.*

Abstract:

Data security is the main concern in different type of applications from data storing in clouds to sending messages using chat. In order to provide security for data in cloud there are many types of techniques which are already proposed like AES, DES, RSA but in existing methods most of the time only single type of encryption was used either AES, OR DES, OR RSA based on user requirement but in this system main problem is each encryption is done using encryption keys if these keys are exposed in any case entire data is lost so we need effective method which can provide more security so in this project hybrid cryptography is used where existing encryption methods are used but three methods will be used.

When user uploads data will split in to three parts and first part will be encrypted using AES , second part will be encrypted using DES, third part will be encrypted using RSA and these three encrypted files will be stored in cloud and keys used for AES, DES and RSA are stored in image using LSB steganography when use want to download total data from cloud first keys should be retrieved from image and these keys are used for decrypting data again by using AES, DES and RSA and final data is combined and stored in file. This method provides more security for data.

Keywords: Cloud Security, AES, DES, RSA Encryption, Data Security

1. INTRODUCTION

There are different factors that cause traffic accidents. Among the most common factors that increase the probability of their occurrence are the geometry of the road, the climate of the area, drunk drivers, and speeding. These accidents can cause harm to the people involved and, although most of these present only material damage, each one affects people's quality of life in terms of both traffic mobility and personal safety. Thanks to technological advances, video cameras have become a resource for controlling and regulating traffic in urban areas. They make it possible to analyze and monitor the traffic flowing within the city. However, the number of cameras needed to perform these tasks has been increasing significantly over time, which makes control difficult if automation mechanisms are not implemented because the number of professionals needed to comply with all the points also increases. Several approaches have been proposed to automate tasks within the control and follow-up process. An example of this is a system based on video camera surveillance in traffic. Through these, it is possible to estimate the speeds and trajectories of the objects of interest, with the objective of predicting and controlling the occurrence of traffic accidents in the area. The scientific community has

presented different approaches to detect traffic accidents. These include statistics-based methods, social network data analysis, sensor data, machine learning, and deep learning.

Deep learning techniques have shown high performance in a large number of problems, especially for image understanding and analysis. These layers exploit the spatial relationship that the input data possess and that, due to the size of the information, it is not possible to achieve with dense neural networks. The use of convolutions on input data with large number of features makes it possible, among other things, to avoid the problem of the curse of dimensionality. This is a very frequent problem when working with data with high complexity, such as images. Likewise, it is important to highlight that the use of several convolutional layers helps the extraction of relevant visual features within the same dataset, which defines the performance of the network. On the other hand, there are problems where the spatial relationship of the data is not a determining characteristic. In some problems, the temporal relationship that the data may have greater importance.

This is because there are events that depend on past and/or future events, that is, on a context of the event in time in order to understand the real event. This is why a new deep learning model has emerged: recurrent neural networks. These networks have a similar architecture to dense artificial neural networks but differ in that at least one neuron has a connection to itself. This allows them to be able to remember what has been previously processed, i.e., it gives them the ability to store information over periods of time (data memory).

.

1.1 OBJECTIVE

The proposed model is liable to meet the required security needs of data center of cloud. AES, DES and RSA are used for the encryption of file slices takes minimum time and has maximum throughput for encryption and decryption from other symmetric algorithms. The idea of splitting and merging adds on to meet the principle of data security. The hybrid approach when deployed in cloud environment makes the remote server more secure and thus, helps the cloud providers to fetch more trust of their users. For data security and privacy protection issues, the fundamental challenge of separation of sensitive data and access control is fulfilled. Cryptography technique translates original data into unreadable form. Cryptography technique is divided into symmetric key cryptography and public key cryptography. This technique uses keys for translate data into unreadable form. So only authorized person can access data from cloud server. Cipher text data is visible for all people.

2. OVERVIEW OF THE SYSTEM

2.1 Existing System

- In existing system cloud used to use any one of the encryption techniques and keys verification is done using identity of user.
- Based on application requirement different encryption techniques are used.

2.1.1 Disadvantages of Existing System

- Only single encryption techniques are used and keys are not managed effectively there are changes of leakage of keys.

2.2 Proposed System

In order to improve security for cloud data compare to existing techniques where keys are shard security between users new hybrid cryptography technique is proposed where three types of encryption are used AES, DES and RSA and LSB steganography technique is used for secure key sharing.

2.2.1 Advantages of Proposed System

- Data is split in to three parts and each part is encrypted using one encryption technique and keys are shared securely by embedding in image.

3. Architecture

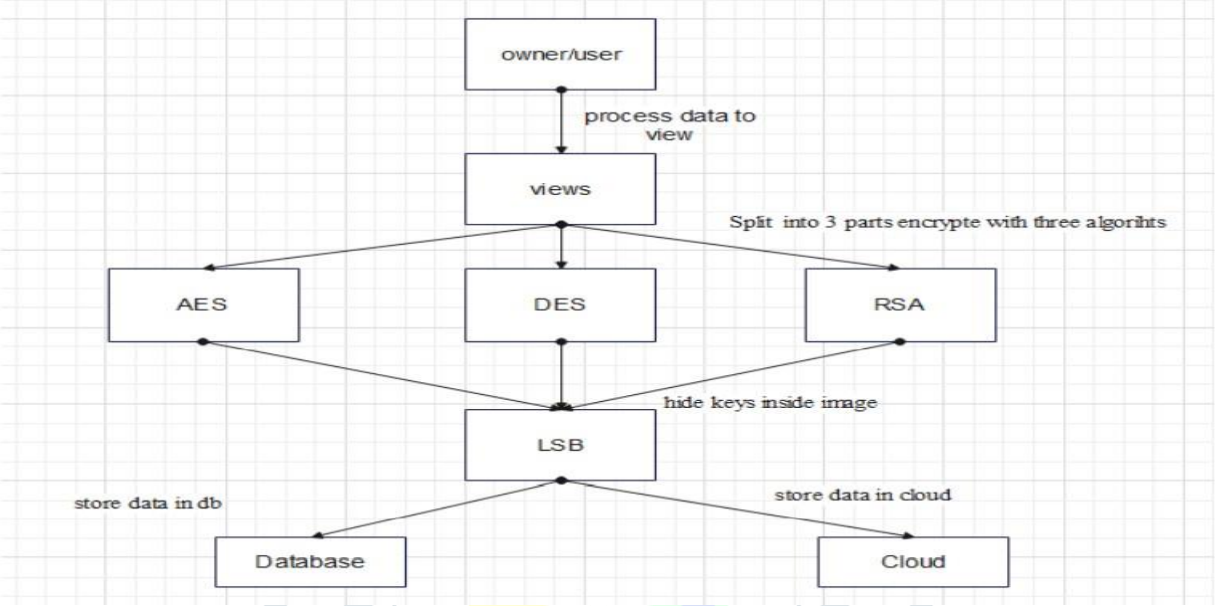


Fig 1: Architecture diagram

4. Design

Owner Module:

Owner will register into the application by providing all the necessary details and therefore he can login into the application using username and password and user can upload the files to cloud and share with the other registered users. He can also view the files uploaded by him and can also view the requests for secret key from the other users and we can respond and the key will be sent to user by mail. Using that key, he can download the file and view the information.

Owner can register with application and these details are stored in SQLite database and owner can login to application with valid username and password.Owner has option to upload files in this process in back-end data is split in to three parts and each part is sent to respective class and returned with encrypted data. This data is stored in database and cloud server. Owner can view requests and respond to request and view files.

User Module:

User will register with application and get username and password. Owner can see all encrypted files uploaded by all users and send request to respective user and get approval to download data and three keys for AES, DES, and RSA are shared to owner email which can be used for owner download.

. User can register with application login with valid username and password and view files upload by other owners. User can see owner name file type and encrypted data if user want to download data user sends requests to user who will get response if user sends security keys. User can download by using these three keys and in the back end theses keys are verified by the keys hidden in the image using LSB algorithm

5. RESULTS SCREEN SHOTS

Owner Home page:

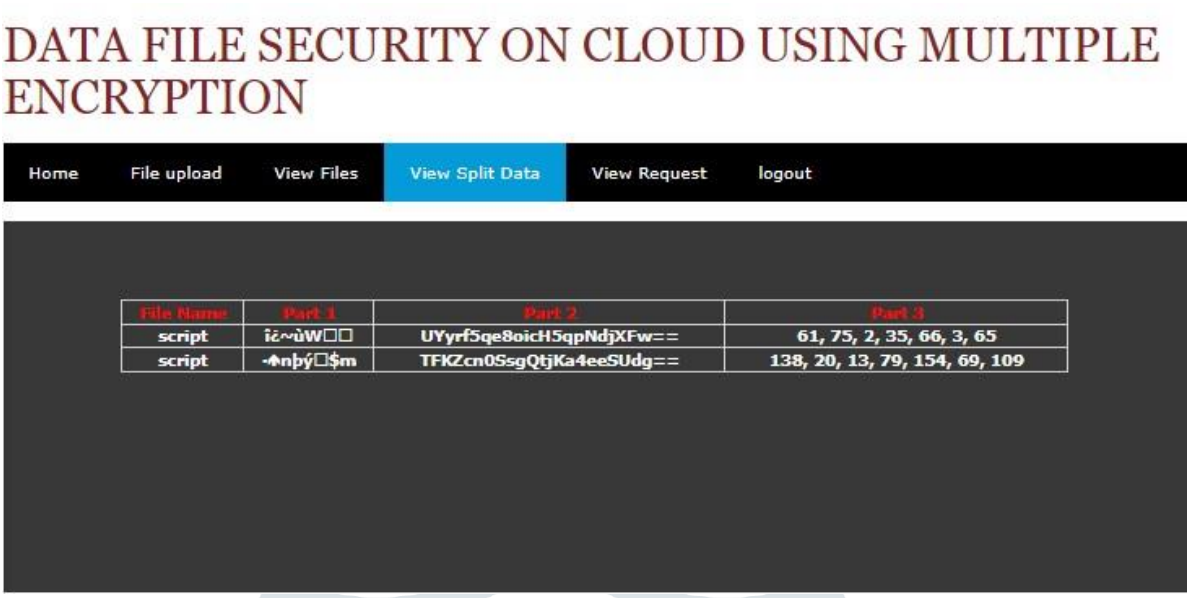
This page is displayed to owner when owner logins to application.
Owner can view all options on menu.

File Upload Page:

This page is displayed to owner when file upload option is selected from menu options. Using this option owner can select file and upload to database.

Owner View Files:

View Split Data:



Owner selects view split data to see each encrypted part of data.

View Requests:

:

User Home Page:

User View Files Page:

User View verified Data:

Verify DES part 1 Key:

Verify AES Part 2 Key:

Verify RSA Part 3 Key:

6. CONCLUSION

The main goal is to securely store and access data in cloud that is not controlled by the owner of the data. We exploit the technique of AES, DES, RSA cryptography encryption to protect data files in the cloud. Two part of the cloud server improved the performance during storage and accessing of data. These Encryption algorithms used for encryption is another advantage to improve the performance during encryption and decryption process. We assume that this way of storing and accessing data is much secure and have high performance. Our efforts are going on to solve the problem of security issues by using single encryption algorithm of data in cloud computing environment.

FUTURESCOPE:

- It is not possible to develop the system that makes all the requirements of the user. User requirements keep changing as the system is being used. Some of the future enhancements that can be done to this system are:
    - As the technology emerges, it is possible to upgrade the system and can be adaptable to desired environment.
    - It is based on object-oriented design any further changes can be easily adoptable.
- Based on the future security issues and scope, security can be improved using emerging technologies and multi-dimensional application can be developed.
- User can select type of encryption technique and user can select two or three methods based on that each file will have new way of technique.

7. REFERENCES

[1] Peter Mel and Tim Grace, "The NIST Definition of Cloud Computing", NIST, 2010.

[2] Achill Buhl, "Rising Security Challenges in Cloud Computing", in Proc. of World Congress on Information and correspondence Technologies, pp. 217-222, Dec. 2011.

[3]Srinivasarao D et al., "Breaking down the Superlative symmetric Cryptosystem Encryption Algorithm", Journal of Global Research in Computer Science, vol. 7, Jul. 2011

[4] Tingyuan Nye and Tang Zhang "An investigation of DES and Blowfish encryption algorithm" , in Proc. IEEE Region 10 Conference, pp. 1-4 ,Jan. 2009.

[5] Jitendra Singh Adam et al.," Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm" , International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2,Aug. 2012..