SECURE FILE STORAGE USING HYBRID CRYPTOGRAPHY

Dr.M.Rajaiah, Dean Academics & HOD, Dept of CSE, Audisankara College of Engineering and Technology, Gudur.

Mr. S. M. Rafi, Assistant Professor ,Dept of CSE, Audisankara College of Engineering and Technology, Gudur.

Ms. K. Yasaswetha, UG Scholar, Dept of CSE, Audisankara College of Engineering and Technology, Gudur.

Mr. K. PardhaSaradhi, UG Scholar, Dept of CSE, Audisankara College of Engineering and Technology, Gudur

Mr. G. Jayanth, UG Scholar, Dept of CSE, Audisankara College of Engineering and Technology, Gudur

Ms. K.Lakshmi Prasanna, UG Scholar, Dept of CSE, Audisankara College of Engineering and Technology, Gudur

ABSTRACT _ Cloud is used in various fields like industry, military, college, etc. for various services and storage of huge amount of data. Data stored in this cloud can be accessed or retrieved on the users request without direct access to the server computer. But the major concern regarding storage of data online that is on the cloud is the Security. This Security concern can be solved using various ways, the most commonly used techniques are cryptography and steganography. But sometimes a single technique or algorithm alone cannot provide high-level security. So we have introduces a new security mechanism that uses a combination of multiple cryptographic algorithms of symmetrickey and steganography. In this proposed system 3DES (Triple Data Encryption Standard), RC6 (Rivest Cipher 6) and AES (Advanced Encryption Standard) algorithms are used to provide security to data. All the algorithms use 128-bit keys. LSB steganography technique is used to securely store the key information. Key information will contain the information regarding the encrypted part of the file, the algorithm and the key for the algorithm. File during encryption is split into three parts. These individual parts of the file will be encrypted using different encryption algorithm simultaneously with the help of multithreading technique. The key information is inserted into an image using the LSB technique. Our methodology guarantees better security and protection of customer data by storing encrypted data on a single cloud server, using AES, DES and RC6 algorithm.

Keyword— Cloud Computing and Storage, AES Algorithm, RSA Algorithm, Blowfish Algorithm.

1.INTRODUCTION :

Cloud computing is originated from earlier large-scale distributed computing technology. NIST defines cloud computing as a model for enabling convenient on demand network access to a shared pool of configurable computing resources (like network, storage, application and services) that can be quickly provisioned and released with minimal management effort or service provider interaction.

In Cloud computing files and software are not fully contained on the user's application and Program are residing in provider premises. The cloud provider can solve this problem by encryption the files by using encryption algorithm. This paper presents a file security model to provide an efficient solution for the basic problem of security in cloud environment. In this model, hybrid encryption is used where files are encrypted by file splitting and RSA is used for the secured communication between users and the servers.

2.LITERATURE SURVEY :

The above mentioned paper propose the way of splitting files into different parts and then applying the hybrid cryptography for each part.

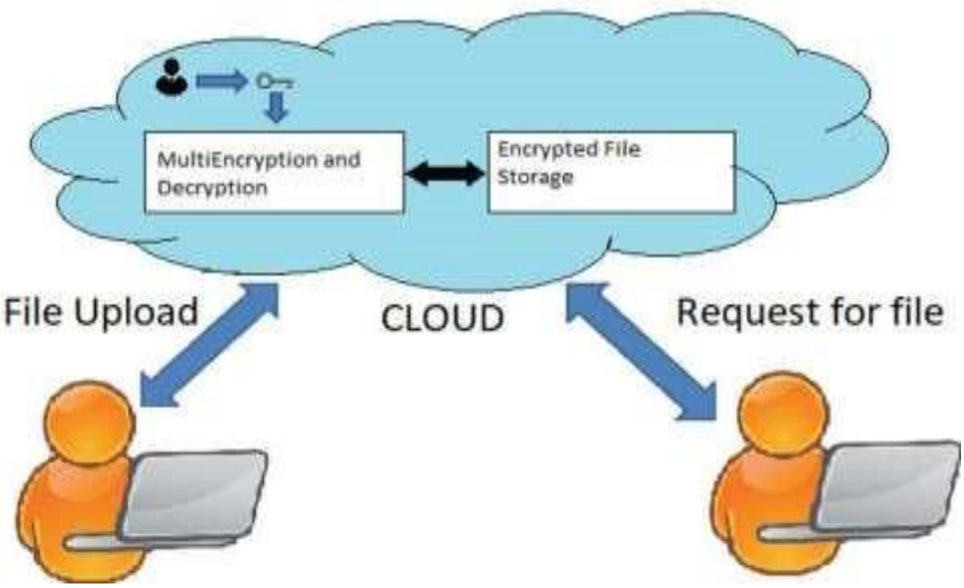
The method uses LSB steganography method for storing keys anduses symmetric cryptographic algorithm for encryption and decryption.

3.PROPOSED SYSTEM :

In our system cloud owner upload the data on the cloud server .To enhance security of file in cloud computing source file is break into different parts.

Every part of file is encrypt using encryption algorithm .Encrypted file is stored on cloud database server .

Cloud server contains only a single part of a particular file of any format uploaded by user which ensures that if any attack take place no important data is encrypted. The files that are selected for upload by the user will be encrypted atthe client side before uploading and decrypted after the user downloaded it.



Advantages:

- The stored image file is completely secured, as the file is being encrypted not by just using one but three encryption algorithm which are AES, DES and RC6.

- The key is also safe as it embeds the key in image using LSB.

- The system is very secure and robust in nature.

As in the above figure, the files that the user will upload on the cloud will be encrypted with a user-specific key and store safely on the cloud.

1.User Registration

For accessing the services the user must first register yourselves. During the registration process various data like Name , username, password, email id, the phone number will be requested to enter. Using this data the server will produce unique user-specific keys that will be used for the encryption and decryption purpose. But this key will not be stored in the database instead it will be stored using the steganography algorithm in an image that will be used as the user's profile picture.

2. Uploading a File on Cloud

- When the user uploads a file on the cloud first it will be uploaded in a temporary folder. Then user's file will be split into N parts.
- These all parts of file will be encrypted using cryptographic algorithms. Every part will use a different encryption algorithm.
- These all parts of file will be encrypted using different algorithms that are AES, 3DES, RC6. The key to these algorithms will be retrieved from the steganographic image created during the registration.
- After the split encryption, the file reassembled and stored in the user`s specific folder. The original file is removed from the temporary folder.
- Then Combining all Encrypted Parts of file.

3. Download a File from the Cloud

- When the user requests a file to be downloaded first the file is split into N parts.
- Then these parts of file will be decrypted using the same algorithms with which they were encrypted. The key to the algorithms for the decryption process will be retrieved from the steganographic image created during the registration.
- Then these parts will be re-combined to form a fully decrypted file.
- Then file will be sent to the user for download.

3.IMPLEMENTATION :

Another advantage of cloud storage could be additional security. The proposed system aims to make the cloud storage system secure using data encryption. Thus, the aim of the proposed system is to increase security of data uploaded onto the cloud by using encryption algorithms to make the system more secure.

The system is designed such that it works in the following way:

The user signs in if already registered, or signs up to register themselves by providing their details such as name, email id, phone number, password for account etc.

The user then selects the file that is to be uploaded by browsing from local storage.

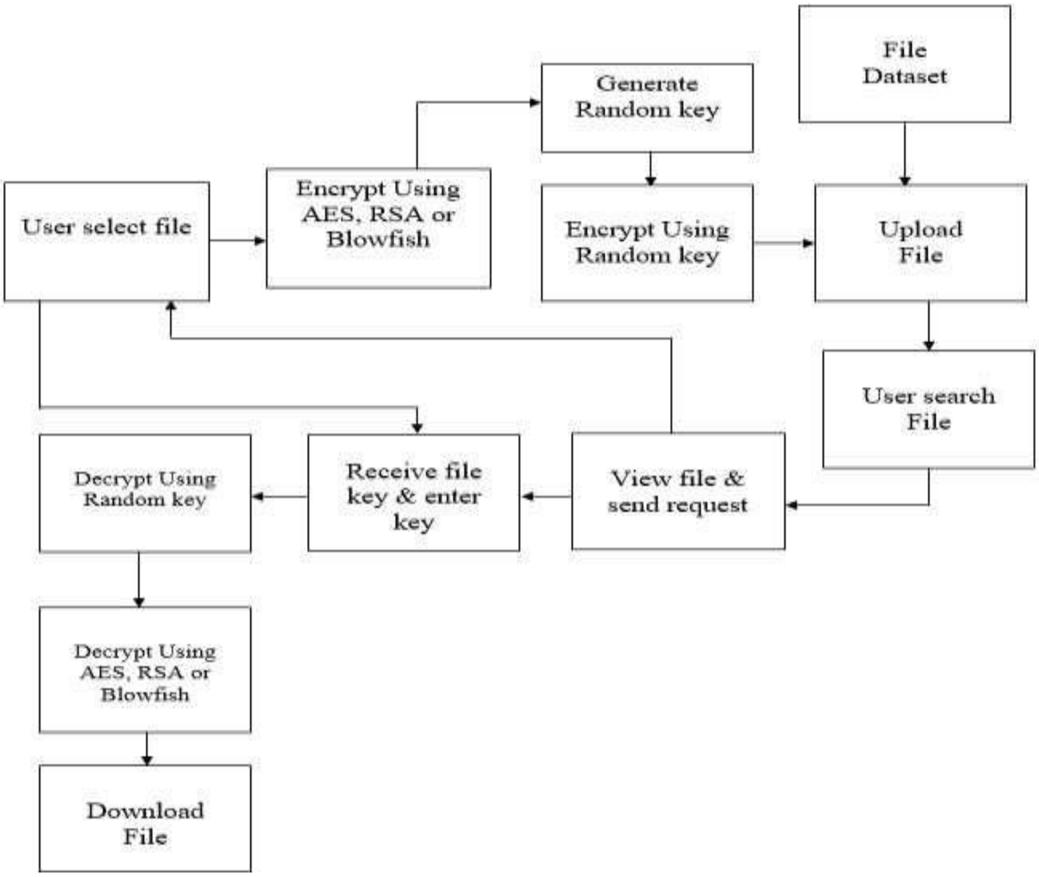
The user then selects the encryption algorithm that they want to use. The proposed system provides the choice between using a combination of AES and RSA or AES and Blowfish.

The selected file gets uploaded after getting encrypted using the selected encryption algorithm combination.

The user also has the option of viewing the files that they have uploaded or have access to and downloading them.

On selecting a file to download it, the user is sent the decryption key on their email id that was entered on registration or sign-up. Using this key, the user can download the decrypted or original file.

The system also provides a comparison with respect to security between the two hybrid encryption algorithm combinations i.e. AES and RSA hybrid combination and AES and Blowfish combination.



4.CONCLUSION :

The main aim of this system is to securely store and retrieve data on the cloud that is only controlled by the owner of the data. Cloud storage issues of data security are solved using cryptography and steganography techniques. Data security is achieved using RC6, 3DES and AES algorithm. Key information is safely stored using LSB technique (Steganography). Less time is used for the encryption and decryption process using multithreading technique. With the help of the proposed security mechanism, we have accomplished better data integrity, high security, low delay, authentication, and confidentiality. In the future we can add public key cryptography to avoid any attacks during the transmission of the data from the client to the server.

REFERENCES :

1. J. Howell. Number of Connected IoT Devices Will Surge to 125 Billion by 2030, IHS Markit Says. https://technology.ihs.com, Accessed June 2019.
2. V. Balasubramanian, et al. . A Mobility Management Architecture for Seamless Delivery of 5G-IoT Services. ICC 2019 - IEEE International Conference on Communications (ICC). 2019; 1-7.
3. Al Ridhawi, Ismaeel, et al. . A Profitable and Energy-Efficient Cooperative Fog Solution for IoT Services. IEEE Transactions on Industrial Informatics. (2019).
4. N. Abbas, et al. .A Mechanism for Securing IoT-enabled Applications at the Fog Layer. J. Sens. Actuator Netw. 2019; 8(1):16.
5. SonicWall Inc. . 2019 SonicWall Cyber Threat Report (2019). https://www.sonicwall.com, Accessed June 2019.
6. D.E. Kouicem, A. Bouabdallah, H. Lakhlef. Internet of things security: A topdown survey. Computer Networks.2018;141:199-221.
7. N. Tariq, et al. The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey.2019;19(8): 1788.
8. J. Canedo, A. Skjellum. Using machine learning to secure IoT systems, in Proc. 14th IEEE Annu. Conf. Privacy Security Trust (PST). 2016:219-222.
9. M. AL-Hawawreh, N. Moustafa, E. Sitnikova. Identification of malicious activities in industrial internet of things based on deep learning models. Journal of Information Security and Applications. 2018;41:1-11.
10. M. Asad, et al. .DeepDetect: Detection of Distributed Denial of Service Attacks Using Deep Learning. The Computer Journal. 2019;0(0).

11. M. Aloqaily, S. Otoum, I. AlRidhawi, Y. Jararweh. An intrusion detection system for connected vehicles in smart cities. Ad Hoc Networks. 2019.

12. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao. A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things J.2017;4(5):1125-1142.

AUTHOR PROFILES

Dr.M.Rajaiah , Currently working as an Dean Academics & HOD in the department of CSE at ASCET (Autonomous), Gudur, Tirupathi(DT).He has published more than 35 papers in, Web of Science, Scopus Indexing, UGC Journals.

N Anil Kumar Chowdari M.Tech Assistant Professor Audisankara College of Engineering & Technology Gudur

Ms. K. Yasaswetha, UG Scholar, Dept of CSE, Audisankara College of Engineering and Technology, Gudur.

Mr. K. PardhaSaradhi, UG Scholar, Dept of CSE, Audisankara College of Engineering and Technology, Gudur

Mr. G. Jayanth, UG Scholar, Dept of CSE, Audisankara College of Engineering and Technology, Gudur

Ms. K.Lakshmi Prasanna , PG Scholar, Dept of CSE, Audisankara College of Engineering and Technology, Gudur

.