Eliminating Risks in Uploading and Downloading Files from Cloud Using Steganography and Cryptography Techniques

R. Senthilkumar, Jyothi Joy, Dhanabagyam. G., Alex Jeeva J. J.

Department of Computer Science and Engineering, SNS College of Technology, Anna University, Coimbatore, Tamil Nadu India

ABSTRACT

Cloud computing is most popularly used in everywhere like IT field, research areas and medical filed etc. The users can retrieve data from the cloud using request method. To storing the data within the cloud we are facing a lot of problems to overcome those problems we used different methodologies. Cryptography and Steganography techniques are we most commonly used for the security purpose. In the proposed system, we introducing a lot of algorithms like AES, BLOWFISH, RC6 and BRA algorithms. These algorithms are used in the block-wise security. In the proposed system the data which we uploaded in the cloud will be split into block and each block will contain 178 characters. The data will be split into blocks and encrypting the data using this algorithm.

Keywords: Encode, Decode, Cryptography, Steganography.

I. INTRODUCTION

Cryptography will translate the original document into an encrypted format which is not understandable to users. The Cryptography process will be divided into two type public key and symmetric key. In this process first will convert the original data into cipher text and we are encrypting the data the cipher text will be visible to everyone. AES, DES, IDEA, and BRA this algorithm are used in the symmetric key Cryptography. In the proposed system we are using the key method to provide security. This algorithm will Provide the security very less and it will take less time to encode and decode the data. RSA and ECC algorithms are used in the public key algorithm method. These algorithms are taken more time to encode and decode the data but it will provide more security. Steganography is the process of hiding the data with in image or video. The data within the image will not be visible to external viewers. The user who did the process he only can understand data and this is used for the high-security process. The data add to the cover file after that it will look like a normal image. By using public key only the users can extract the data from the image. The public key will be only aware to sender and receiver. Steganography needs more space to store the data that is the main advantage of this technique.

Another technique is symmetric key in this key we using a single key for encoding and decoding the data. A 128-bit key is used in the symmetric key and the steps of the symmetric key will execute randomly. So the users can’t easily identify the process. DES algorithms used in the encoding and decoding the size of the key used in the DES are 112 bit. The main drawback of DES algorithm is a key size less. AES and 3DES algorithms are merged into a hybrid algorithm to accomplish confidentiality. It is harder for an attacker to recover a secret file of the user. It consumes the maximum amount of delay to translate data into decode and encode form.

In existing system single algorithm is used for data encode decode purpose. But the use of the single algorithm is not accomplished high-level security. If we use single symmetric key cryptography algorithm than we have to face security problem because in this type of algorithm applies a single key for data encode and decode. So key transmission problem occurs while sharing key into the multiuser environment. key cryptography algorithms accomplish high security but the maximum delay is needed for data encode and decode.

Security Measures

1. Data Uploaded in Cloud
2. Data Downloaded from Cloud

To solve above Security is one of the most difficult tasks to implement in cloud computing. The paper basically deals with the security issues that are experienced during the storage of data on the cloud. The cloud vendors generally store the client's data and information in the cloud without following any Almost every cloud provider does not provide enough security measures to ensure the data safety and that's why clients waver keeping their data at some place which is very easy to be accessed by someone else. Proposed System The proposed system is implemented in Eye so that is one of the cloud providers. In order to apply security features, a hybrid encryption technique using the AES and RSA algorithms is used where 128 bit secret key for AES and 1024 bit key for RSA is used. Upload option leads to a generation of RSA public key-n, RSA public key-e,RSA private key-d and AES secret key, user will require saving the RSA private key and AES secret key, As soon as user tries to upload the data on cloud, the data is first stored in a temporary directory and after calling AES and RSA algorithm, requiring the user to enter the AES secret key the file will get stored in the database permanently corresponding to the user account.The temporary file gets deleted. Now, when the user wants to access the data stored in cloud or wants to download the data, it goes through the download procedure whereby user has to specify the filename to be downloaded and has to provide the AES secret and RSA private key which is kept secret by the user and is known only to him.

II. METHODS AND MATERIAL

Wireless sensor the proposed system basically consists of two modules
(I) Upload Module
(II) Download Module

Upload Module:
It consists of four parts

(i) Authentication:
The user authenticates himself to the Cloud With his unique username and the password.

(ii) Upload
This module allows the user to upload his files in a secure way. Uploads the encrypted form of that data (file) in his document directory of cloud through this gateway.

(iii) Ky Generation
A key generation is based on system timing.

(iv) Encryption
The data after uploading is first stored in the Temporary file of the server that is in the Cloud. Then encrypt the data by using the public key of the user and stores the encrypted form of data in the documents of the user. The temporary files are then unlinked.

Download Module
It consists of two parts

(i) Decryption
When the user wants to download his secure data, he is prompted to enter his user name along with the secret private key. By using the private key of the user the cloud decrypts the data.

(ii) Download
Cloud send the Decrypted data to the user Thereby giving the user his original data.

III. RESULTS AND DISCUSSION

A This paper proposed a hybrid encryption algorithm using RSA and AES algorithms for providing data security to the user in the Cloud. The biggest advantage it provides us is that the keys are generated on the basis of system time and so no intruder can even guess them there by giving us increased security along with convenience. Private Key and the Secret key is only known to the user and therefore user's private data is not accessible to anyone not even the Cloud's Administrator. The main purpose behind using RSA and AES encryption algorithm is that it provides three keys i.e. public key for Encryption, and private key and secret key for decryption. The data after uploading is stored in an encrypted form and can be only decrypted by the private key and the secret key of the user. The main advantage of this is that data is very secure on the cloud.

IV. CONCLUSION

By using this proposed model a secure path can be established for communication. The system provides security at different point in time starting from cluster head election (SLEACH), secure data transfer through session establishment CKM with inclusion of pairwise key establishment (RCD and RMCM) in case of intra-cluster communication and triple key establishment in case of inter-cluster communication and watchdog nodes with rules definition and KDD data set. Hence, as a system it provides a different layer of security and monitoring. Certain rules for internal attackers have been defined in the model. The KDD dataset has been used as a protective measure in the model. The KDD dataset can be well trained and implemented in the future so that a better-secured system can be implemented. Also with respect to key distribution and establishment randomized combinatorial design theory and Markov chain model has been used. RMCM is surely granted security in terms of key distribution but further improvements can be made on successful key generation rate.

V. REFERENCES

[1] Prof. Vishwanath S. Mahalle, "Implementing RSA encryption algorithm to enhance the data security of cloud in cloud computing", International journal of pure & applied research in engineering and technology, 2013, volume 1(8):220-227, ISSN-2319-507X IJPRET.

[2] Uma Somani, Kanika Lakhani, Manish Mundra "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security Of Cloud in Cloud Computing" 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC) – 28-30 Oct, 2010 IEEE.

[3] (U.S.) Nicholas. Carr, fresh Yan Yu, "IT is no longer important: the Internet great change of the high ground - cloud computing," The Big Switch: Rewining the World, from Edison to Google , CITIC Publishing House, October 2008.

[4] Ya-Qin Zhang, the future of computing in the "cloud-Client", The Economic Observer reported, http://www.sina.com.cn, 2008 Nian 07 Yue 12 Ri