© 2016 IJSRST | Volume 2 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Technical - Review

Implementation of Multi-Party Key Authentication and Steganography for Secured Data Transaction in Cloud

V. Shalini, E. Sreeja, M. Veluchamy

Department of Information Technology, Dhanalakshmi College of Engineering, Chennai, Tamiladu, India

ABSTRACT

Cloud security is effective only if the correct defensive implementations are in place. Efficient cloud security architecture should recognize the issues that will arise with security management. Cloud providers either integrate the customer’s identity management system into their own infrastructure. We propose an identification system which links the confidential information of the users to store in an encrypted fashion using steganography. Implementation of multi-party key authentication and steganography for secured data transaction in cloud provides the users with security for their data stored in the collaborative environment in a reliable fashion.

Keywords : Steganography, Merkel Hash Tree, Multi Party.

I. INTRODUCTION

The main aim of this paper is to provide a secured data transaction based on hiding a mutual key in an image using steganography technique, basically steganography technique focuses on encrypting the image but here we use specific algorithms to generate the keys which will be used while authenticating the user and then get an access which will grant the data user to get their desired file from the cloud server.

Here we are performing another activity as creating an application in the cloud server using our Google account to store our data more securely in the cloud server each user login and actions performed by the user will be stored in that application in an encrypted format using merkel hash tree algorithm in which data will be integrated and stored using a tree format.

Existing Work

In the existing system, security solutions mainly focus on the authentication cannot be illegally accessed, but neglect a tenuous privacy issue (i.e.) it mainly provides security only for authentication and does not take care of the very tiny issues in the system, as a result a very less security is provided in which the users data can be accessed very easily by the hackers and the content can be changed very easily and hereby they are missing their privacy by which some anonymous request can get all the data from cloud and share them in the collaborative environment. In this case the authorized user should be provided subtle privacy towards their data.

Proposed Scheme

In this proposed system, there will be three entities users, cloud server & trusted third party (TPA). Data users are both data owners & data users. Every user will be registering with the cloud Server. Cloud will be generating pair wise keys, primary and secondary keys for both cloud server & data user. users 1 wants to access the data of users 2 then shared keys are generated and accordingly the data is authorized for usage. As a modification process, an access key is generated while registrations with cloud after that only shared key are generated. Finally a mutual access key is generated by the data owner to the data user without the interaction of the cloud server by using the data owner and the data users mutual understanding and sent via Email or else the data owner can also ignore the request .In case of providing acceptance to the request, the data user will have to hide that mutual key in an image called steganography and sent to the data owner. Data is accessed by only after verifying mutual key using destaganography and as a result the requested user will be able to view the requested file.

II. METHODS AND MATERIAL

Experimental Work

A. Creating an Application in Cloud

In this work as an initial process the data owner has to create an application in the cloud server using their cloud ccount (they can use any type of cloud such as amazon, one cloud, google drive etc.) here we are using drop box account to create an application in cloud. While creating that application in cloud an app key and a secret key will be generated and those keys will be used to connect our cloud application with our external application which will be visible to the data user.

B. Uploading File Using the Application

This uploading process can be carried out by either data owner and data user who wants to upload the file content into the application, while the user registration into the application by using their user name and password and some specific parameters they will be provided a public key which will plays a main role while uploading of file, the users with the public key can only upload the file into the application. While uploading a certain steps should be carried out first they should browse an image file which is used to steno the file content, and as the second step should browse the file ontent which is very important to be uploaded with much security and as the next step an index key word should be provided for that certain file which will be useful while searching the file for downloading.

C. Downloading the File

While if the data owner as well as data user wants to download any file from the application they must get login into the system and then they start search for the file they need using the key word if any files are found regarding the given key word the system will display the filename and then user will proceed to download the cloud server will asks for the shared key the user will give no and now the cloud server will take any two bits from the data owners primary key and secondary key as well as any two bits from the data users primary and secondary key combines those keys and generate a shared key and sends to the correct requested users mail id with use of trusted third party verification and then the user will provide the shared key plus access key to cloud server and it will proceed to give request to the file.

D. View Request

The data owner will be able to see the request with the status provided for in his account as request is pending either to provide the service or to discard the request, if the owner wants to approve the request the owner will enter a mutual key and browse the image from the server which is stored in an encrypted format using AES algorithm and mutual key is steganography inside the image and sent to the user mail, the user will then decrypt the image and destegano the mutual key and the user will give that to the server and then the cloud server will separate the content file and the image file and then now the user can view the file.

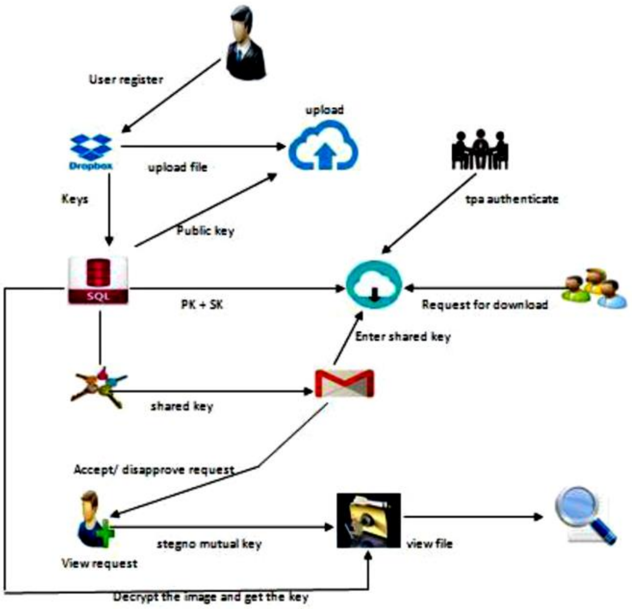

Figure 1. Architecture Diagram

III. RESULT AND DISCUSSION

1. Techniques

A. AES Algorithm

Advanced Encryption Standard is mainly used to encrypt a confidential text into a decryptable format, for example when you need to send sensitive data in e-mail the decryption of the encrypted text it is possible only if you know the right password. AES was designed to be efficient in both hardware and software and supports a block length of 128 bits and key length of 128, 192, 256 bits. It works at multiple network layer simultaneously, AES is one of the most frequently used and most secure encryption algorithm available today. The algorithm is based on several substitutions, permutations and linear transformations, each executed on data blocks of 16 byte-therefore the term block cipher. Those operations are repeated several times, called “rounds”. During each round, a unique round key is calculated out of the encryption key and incorporated in calculations. Based on the block structure of AES, the change of single bit, either in the key, or in the plaintext block, results in a completely different cipher text box. Therefore, AES remains the preferred encryption standard for governments, banks and high security systems around the world.

The behavior of the graphs shows that for file size up to 1000 kb, the required is less and it gradually rises when the file size is increased. If the encryption and decryption time is compared with similar systems, it shows that time required by AESS System is significantly less.

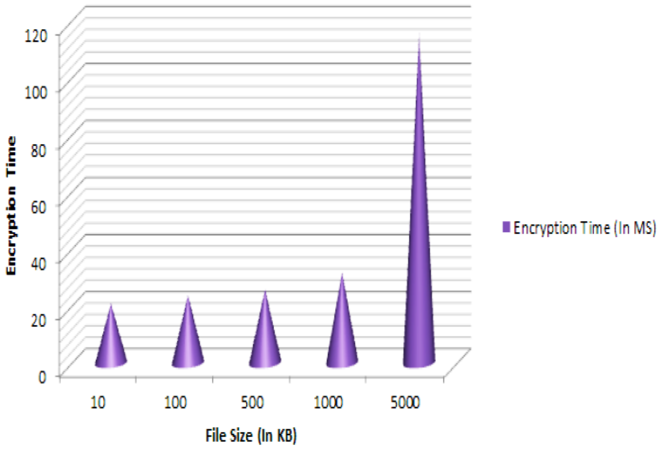

Figure 2. AES Encryption Time Chart

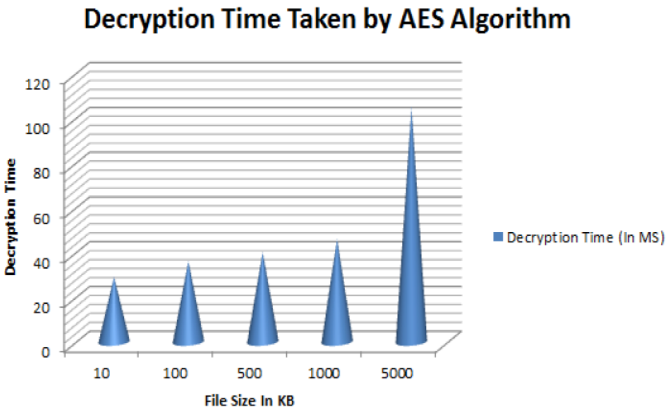

Figure 3. AES Decryption Time chart

B. Steganography

Steganography is a practice of concealing a file, message, image or video within another file, message, image, or video. Generally, the hidden messages appear to be(or be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden messages may be in invisible link between the visible lines of a private letter. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include Stenographic coding inside of a transport layer, such as document file, image file, program or protocol. Media files are ideal for stenographic transmission because of their large size.

For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

C. Merkel Hash Tree

Merkel Hash Tree is a well-studied method which is used for authentication structure. It is used efficiently and also proved that set of elements are stayed undamaged and unaltered. It provides great help in server time reduction. It is used by the cryptographic methods to authenticate the file in blocks.

The leaf nodes of the Merkel Hash Tree are the original hash values of file blocks. The idea behind generating MHT is to break the content file into a number of blocks and get combined iteratively. Now, rehashing the result hash nodes and combine like a tree-like fashion and repeat the same procedure till we get a tree with a single root. The MHT is generated by client and get stored at both client and server side.

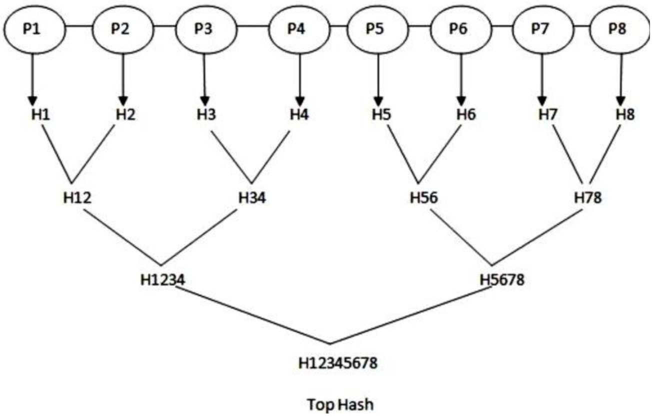

Figure 4. Merkel Hash Tree Structure

D. Key Generation

Key generation is a technique which is used to store the data in a different methodology and mainly the public key algorithm known as RSA plays a vital role in key generation technique such as single shared key uses symmetric key algorithm through which data will be stored very secretly. Since the public key algorithm uses two keys namely public and a private key and that public key is made as visible to one end user so that they can use that public key to encrypt the data and another end user can decrypt the data using their private key. In some conditions they keys have been generated using Random Number Generator technique, and it is very efficient that the hacker cannot easily guess the keys and provides a strong security.

2. Performance Analysis

The existing system of shared based authentication protocol was done by using Attribute Based Encryption of some drawbacks and those where rectified using Advanced Encryption Standard. In the ABE the latency of execution time is comparatively slow when compared to AES. That drawback is rectified by using AES.

Table 1. Comparison of AES and ABE

FEATURES	AES	ABE
Cost incurred	Cost effective	Expensive
Security Rate	Excellent	Comparatively less
Execution time	More fast	Comparatively Slow
Key length	Upto 256 bits	128 bits

And the security rate is comparatively high when compared to ABE, The cost is also considered as a constraint, in which the existing idea uses the logarithm for encryption but here we use keys for both encryption and decryption.

IV. CONCLUSION AND FUTURE ENHANCEMENT

In this work, we have identified a new privacy challenge during data accessing in the cloud computing to achieve privacy-preserving access authority sharing. Authentication is established to guarantee data confidentiality and data integrity. Data anonymity is achieved since the wrapped values are exchanged during transmission. User privacy is enhanced by anonymous access requests to privately inform the cloud server about the users access desires. Forward security is ealized by the session identifiers to prevent the session correlation. It indicates that the proposed scheme is possibly applied for privacy preservation in cloud applications. And as future enhancement, while storing the data into an image using steganography and that image data is integrated into several parts, in such cases if any one part of data is cracked an immediate notification will be sent to data owner through the mail. And so the data owner can prevent the hacking immediately.

V. REFERENCES

[1] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717-1726, http:// ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6311398,Sept. 2013.

[2] R. Moreno-Vozmediano, R.S. Montero, and I.M. Llorente, "Key Challenges in Cloud Computing to Enable the Future Internet of Services,"IEEEInternet Computing,vol.17,no. 4,pp. 18-25,http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6203493,July/Aug.2013.

[3] A. Mishra, R. Jain, and A. Durresi, "Cloud Computing: Networking and Communication Challenges," IEEE Comm. Magazine, vol. 50, no. 9, pp. 24-25, Sept. 2012.

[4] H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Trans. Services Computing, vol. 6, no. 4, pp. 551-559, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6357181, Oct.-Dec. 2012.

[5] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231-2244, Dec. 2012.

[6] J. Chen, Y. Wang, and X. Wang, "On-Demand Security Architecture for Cloud Computing," Computer, vol. 45, no. 7, pp. 73-78, 2012.

[7] K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," IEEE Internet Computing, vol. 14, no. 5, pp. 14-22, Sept./Oct. 2010.

[8] P. Mell and T. Grance,"Draft NIST Working Definition of Cloud Computing," Nat'l Inst. of Standards and Technology,2009