HIDE ME AND AUTHENTICATE: IMPLEMENTATION OF STEGANOGRAPHY AND MULTI PARTY KEY AUTHENTICATION FOR SECURED DATA TRANSACTION IN CLOUD

Shishir Shivakumar*, Y.Mistica Dhas, G.Vishnu
Student, Faculty of Computing, Sathyabama University, Chennai, TamilNadu, India.
Assistant Professor, Faculty of Computing, Sathyabama University, Chennai, India.
Student, Faculty of Computing, Sathyabama University, Chennai, TamilNadu, India.
Email: shishir812@gmail.com

Received on 04-05-2016
Accepted on 30-05-2016

Abstract

Cloud computing is one of most important aspects of data storage and data accessing in today’s times. Cloud mainly comprises of private and remote servers that manage, store and process data. One of the main issues that cloud computing faces today is with regard to the security and privacy concerns. The transactions that happen in the cloud servers mainly face a threat either on the authorization part or data security during transactions. In this paper we propose to add special security measures for authorization and data transactions. In the proposed work the ideology of steganography is put into use. When any user registers with the cloud server, an access key is given by the cloud server so as to access the cloud servers when required, the user needs to request the specific data owner for access allowance. In this the data owners are the data users. Only once is an access key generated, after that all mutual access keys are generated by the data owner for the data user.

This mutual access key is stored inside of an image by text steganography and thus sent to the data user via email. Once the mutual access key (MAK) is verified by the data owner, the data is opened for access. The data requested by the user is sent to the user embedded into an image using the merkle hash tree (MHT) approach in which the particular given function is divided into eight parts and an unknown hash value is added to each of the functions, this also uses steganography. The data is recovered by the user end by decrypting the function using desteganography. This way the data owner achieves data security and the issue of privacy is also taken care of.

Keywords – cloud deployment, steganography, privacy, key generation.
Introduction

Cloud computing refers to the virtual storage and management of data using local servers. In today’s world everything is related to information technology and most of the data is technical along with computer based data which calls for the requirement of large storage and process area. The cloud network has become increasingly famous as it is a very feasible option for data storage and processing. The cloud networks boasts of storing very large amounts of data that can only be accessed with the help of an internet connection. The term internet leads to the thought of hackers and various other attackers that tend to intercept important as well as sensitive data that can be stored in the cloud drivers by users. In the cloud networks there is a high chance of risk with the data getting leaked, thus in the proposed system the work concentrates on data security and as well as the data owner’s privacy. Many systems have been developed for the cloud security concerns but this one uses the ideology and concept of steganography. Steganography is used for the embedding of the mutual access key into an image and as well for the data transaction. The mutual access key (MAK) is given by the data owner to the data user. The mutual access key (MAK) is basic text that is embedded into the image and sent to the data user via email. The user receives the encrypted text and decrypts it and thus gains access to the data. The user receives the image which the latter has to desteganograph so as to get the mutual access key. The cloud server generates keys for all users that have registered to the cloud server so that it can be accessed when required. The cloud servers are nothing but virtual servers. They are the same as physical servers but provide a very different approach when compared to physical servers. The mutual access key that is provided by the data owner is nothing but a combination of algorithm of access keys of both user and the owner. Only for the first time during registration is an access key granted by the cloud server and after that all the keys hence generated are mutual keys. Once the user is authorized by the owner then the data that the user has requested is sent by the owner. This data that is sent is also sent using steganography and applying hash functions. We use the merkle hash tree concept to add hash values to the data that is being sent. Merkle tree applies the tree concept that is data is broken down into nodes and these nodes have to be recovered so as to get the data. The data to be sent is instilled into the image and then the merkle hash tree algorithm is applied to it.

The image is broken down into eight parts and each contains unknown hash value that is added to the data. If the data is to be intercepted by attackers, the attackers would not find all the data in one place. The data is sent via an image and the user has to decrypt the image using a key provided by the data owner so as to retrieve all the data without the hash values
The data is hence securely transacted by the cloud server and also the data owner has privacy over his data.

The work has been divided into various categories for better understanding of the cloud network.

**Related work**

In [1], the work basically points out on all the security issues that is being faced by cloud, the work also suggests the usage of a third party control which has been implemented using the a trusted third party which resolves all the authentication related works. [2] Data privacy control has been addressed to in this work, an effective scheme for data sharing as well as privacy related issues. The concept of IBE has been applied (identity based encryption), effective cloud sharing can be achieved with this. The study [3] collects details from success factors and also proposed the authentication to be a key factor in the success of information security in cloud, authentication is one of the foremost modules of the proposed work. The authentication of any user can be in various formats and ways, the work of [4] suggests the use of public key cryptography, the proposed work enhances the use of keys for authentication and other purposes in the cloud network.[5] The work ideology for the access control has been well defined, the work suggests the use of mCL-PKE for achievement of confidentiality of data and data privacy.

The work proposed by nabeel [6] suggests the use of various keys by the key management techniques namely BGKM, the keys are given to the user but not directly, there are some secrets that are given to the user based on the user’s attributes, then the keys are to be derived by the user based on the secrets and some public information, these keys are in a symmetric format.[7] The concept and idea of a trusted third party auditor has been extracted from this particular paper, it suggests that the data should be audited and verified by a auditor and also the HMAC mechanism for the protection and integration of the metadata.

The work [8] suggests the need for privacy control of the data owners and users, the work uses SAPA protocol, in SAPA shared key feature is achieved and this has been applied to the current work by implementing the concept of steganography and also multiple key generation.

**Proposed work**

**Overview**

In the system proposed, there are three packages, one is the data owner, one is the data user and there is the third party auditor. All the three entities are connected and working in combination with the cloud servers. The data owner in the
cloud system may also become the data user at some point of time. The proposed system not only encrypts the key into the image but also the data which is uploaded by the data owner. This system provides with various layers of security, the key undergoes steganography and sent to the entity that requests the data, once the key is sent the data is also uploaded with hash values attached to it using the merkle hash algorithm. The data when downloaded by the user needs to be specified with a key which has been given to the user so that the data is retrieved in the original form without the hash values attached to it. All the entities that want to access the data must register with the cloud server.

Fig 1: System Architecture

Modules

There are seven modules for the system that has been proposed by this system.

1. Registration
2. Cloud deployment
3. Deployment of TPA
4. Access key and shared key generation
5. Mutual key generation
6. Steganography
7. Authentication

We take into consideration module after module. Hence

1. Registration

The most important aspect of any system is the registration process. The user must have registered with the cloud servers so as to access the data of various data owners. The cloud first provides every user with a login identification with which
the user can log into the cloud server as and when required. Based on the request that is given by the user the server will
do the required procedure. All the authentication details of the user is stored with the cloud in a different server.

2. Cloud deployment

All the information on the users is stored and managed by the cloud service provider database. The database is so
maintained that the information about the user is easily accessible as to when required. The cloud server takes into
account the request of the user and assigns it to the resource assigning function which leads to the request being
performed.

3. Deployment of TPA

The Trusted Parity Auditor or the TPA is the member function that audits all the data. The TPA will generate parity bits
and attach it to the data and hence it will develop a signature using the change and response method. If the signature is not
correct and if any changes occur then it will provide an intimidation to the user regarding the changes.

4. Shared key and access key generation

When a user registers with any cloud server, the cloud network itself will provide the user with pair of primary and
secondary keys. The access key is used by the user to access data in the cloud server and to access the cloud network and
the shared key is used by the user to share data with other users or to access data from other data owners. This module is
responsible for the generation of keys in the cloud system.

5. Mutual key generation

In this module we take into the aspect of mutual key generation. The mutual key is such that it is given to the user by the
owner. The owner steganographs this key into an image and sends it to the user who has requested the data. The user
needs to desteganograph the image in order to get the key and access the data.

6. Steganography

Steganography is the method of concealing a secret text or message in an image. It is one of the most effective and oldest
ways of safely passing messages in a system. The basic concept and ideology of steganography is that the message or text
should not be visible to the naked eye.

In the proposed system we use text steganography for message passing that is a text is embedded into a image and sent.
The benefit of text steganography is that it is easier for communication and also cost effective. Various properties such are
number of words, placement of words, number of vowels, number of characters are used during the process of steganography.

7. Authentication

The point of creating this whole module is for the interaction between the data owner and the data user. The data owner needs to authenticate the data user to access the data.

He does this by verifying the user by sending a mutual access key for data access. The user needs to get authenticated by the data owner to get permission to access the data.

Algorithm Description

1. The proposed system makes the usage of various algorithms and the merkle hash tree concept for data and key transaction.

2. There is a usage of the AES algorithm for encrypting the key. The AES algorithm is used for the text, it converts the text into an encrypted data format which cannot be decrypted unless the necessary password or key is used.

3. The AES or Advanced encryption standard is the most widely used and is available for use of all on the internet.

4. F5 algorithm is used for process of steganography that is when the text needs to be embedded into an image. There are steps to be followed when come to the implementation of the f5 algorithm.

- A parameter or constant k has to be defined with regard to the medium’s capacity and the length of the secret message that has to be encoded.

- \[ n = 2^k - 1 \] (equation to calculate the length of the code word.) where n is the length.

- After calculation embedding of the secret text with matrix encoding \((1, n, k)\).

- Suppose we need to embed two bits which we consider to be \(y_1\) and \(y_2\). The bits need to be places in three modifiable bit places which are \(b_1, b_2,\) and \(b_3\).

- \(y_1 = b_1 \oplus b_3, \quad y_2 = b_2 \oplus b_3\) (nothing changes)

- \(y_1 = b_1 \oplus b_3, \quad y_2 = b_2 \oplus b_3\) (b1 changes)

- \(y_1 = b_1 \oplus b_3, \quad y_2 = b_2 \oplus b_3\) (b2 changes)

- \(y_1 = b_1 \oplus b_3, \quad y_2 = b_2 \oplus b_3\) (b3 changes).

- In all of the cases above we do not change more than one bit at a time.
The equation \( n = 2^k - 1 \) determines the change of bit places where \( n \) is the modifiable bit places.

5. We use the merkle hash tree concept for data transaction.

6. The merkle hash tree algorithm is used when the data owner needs to send the user the requested data.

7. The data is embedded into an image using steganography and then the image is split into eight different parts.

8. The embedded data is attached with unknown hash values so that even if hacked data cannot be retrieved. The data is split into 8 parts that is, \((1,2,3,4,5,6,7,8)\).

- Hash value addition:

   There is a hash value that is added to each part of the data. The values being \((1,2;3,4;5,6;7,8)\) the values get separated into 4 pairs with each part having hash functions.

   Further the values get separated in 2 parts \((1,2,3,4;5,6,7,8)\)

9. The values get hash functions and then are transferred to the user who needs to enter a mutual access key which decrypts it into the original state.

**Results and Discussion**

The proposed system has a number of advantages when compared to the later systems. The proposed system follows a orderly fashion such that the key and the data to be sent to the user, both undergo steganography. One of the main issues of privacy is solved in the proposed system; the data owner has full privacy over the data and only shares the data with the user the owner has authenticated. If even suppose the key is hacked by any unknown entity then to the key is stored inside an image hence it becomes difficult for the hacker to access the key. If by any chance there is a possibility of a hacker hacking the key, the data sent by the owner is also steganographed and sent and it can only be accessed with the mutual access key that the owner generates and sends to the user. The data is also attached with hash values using merkle hash tree algorithm so that the data cannot be accessed by any unknown entity.

![Fig 2: Data uploading](image-url)
The data is being uploaded by the data owner into the cloud server. The data is uploaded along with hash values attached to it.

Fig 3: Mutual access key generation

The data when being accessed by any user, the system asks the user for a mutual access key that the user can request from the owner.

Fig 4: Approval of requests

The owner approves the request only if the user is authentic and sends a MAK (mutual access key) to the user via email.

Fig 5: steganography (embedding of key)

The data owner embeds the key into the image and sends it to the user along with a decryption key which is sent via email.

Fig 6: Decryption of image
The data user is intended to enter the decryption key for the image which will provide the user with the mutual access key with which the data can be accessed.

**Fig 7: Data ready to be accessed by the user after authentication.**

Once the mutual access key is gained by the data user, the user gets authenticated and hence the data is open for access to the specific user only.

**Comparative study**

This study shows in particular the graphical representation of various factors discussed such as the privacy, authentication and data integrity. The graph depicts study between the existing system and the proposed system.

**Conclusion**

In the proposed system we have identified a new privacy challenge and worked on it. In the system which we have proposed the authentication of the user is the main goal in hand. The system takes on the privacy and security challenge with various key and authentication protocols. Authentication is put to heavy use for achieving data confidentiality and data authenticity. The user needs and requests are put at top priority by the cloud server. The data owner also has a sense of privacy that the data is only accessed by users that have been authenticated and the data owner and the data user are in communication with each other with the help of keys.
References


Corresponding Author:
Shishir Shivakumar*
Email: shishir812@gmail.com