Securing Data in Cloud Storage by using Steganography and Merkle Hash Tree Algorithm

K. Sasireka, P. Shanthi* and A. Umamakeswari
School of Computing, SASTRA University, Thanjavur, Tamilnadu, India; Infosasi93@gmail.com, shanthip@cse.sastra.edu, aum@cse.sastra.edu

Abstract

Objectives: Cloud computing is incomprehensible creating innovation, the testing issue is the way to successfully share encoded information in cloud computing. Cloud server randomly produces primary, secondary and access keys, after record is made in the server for specific information proprietor. Methods: Data proprietor encodes the record and conceal the data into a picture called steganography. Picture is split and is stored in cloud. Cloud server creates shared key utilizing the primary and secondary keys of data user and data owner in order to avoid unauthorized sharing of data. Data proprietor can share the information to different users by sending mutual key to users by means of e-mail safely. Mutual key is likewise covered into a picture for securing that key. Original information is downloaded strictly to check the mutual key. Findings: The exchange of secret data to the authorized user effectively promotes data confidentiality and integrity. By giving mutual key to the cloud server, the user can see the document. Applications: The method can be applied to share confidential data stored in cloud with small cipher text expansion.

Keywords: Cloud Computing, Data Security, Image Splitting, Key Generation, Steganography

1. Introduction

Cloud computing has recently risen as a promising facilitating stage that permits different cloud clients called inhabitants to share a typical physical registering base. With speedy execution of the considered Software as a Service (SaaS) and Service Oriented Architecture (SOA), the Internet has advanced into a critical administration delivery infrastructure rather than just giving host network. To improve security of data sharing in cloud environment, two major techniques are applied. One is steganography and another one is image splitting. The encrypted file is hidden into an image called steganography. Then that image is split into several parts and stored in cloud storage.

1.1 Steganography

Concealing information into a picture is called steganography. The principle centers of this steganography calculation are the utilization of exchanging mystery message to a content document, compressing record, a key, changing over both compressed document and key into a progression of twofold codes, and the utilization of encoding every last two parallel codes into pixels in picture. The picture quality is still strong where the distortion and shading changes of pictures are decreased to the base or zero-bending. Mystery message, then again, is hard to be stolen. The steganography pictures are favored as cover medium since it won’t get the consideration of a question of investigation. The upside of steganography over cryptography is, though the act of securing the substance of a message alone is cryptography, steganography is concerned with covering the way that a mystery message is being sent, and in addition hiding the substance of the message.

1.2 Merkle Hash Tree (MHT)

For splitting the image, MHT algorithm is used. It is a tree in which each non-leaf hub is marked with the hash of the names or values (if there should be an occurrence

*Author for correspondence
of leaves) of its tyke hubs. Hash trees are helpful on the
grounds that they permit productive and secure confirma-
tion of the substance of extensive information structures.
Hash trees are a speculation of hash records and hash
chains. Exhibiting a leaf hub is a part of the given hash
tree requires handling a measure of information corre-
sponding to the logarithm of the quantity of hubs of the
tree; this appears differently in relation to hash records,
where the sum is corresponding to the quantity of hubs.

Stateless collector case is focused in, where the clients
don't overhaul their state from session to session. They
present a system called the Subset-Cover structure, which
abstracts an assortment of repudiation plans including
some beforehand known ones. Two express Subset-Cover
renouncement calculations utilized here: these calcula-
tions are exceptionally adaptable and work for any number
of denied clients. This instrument does not require from
the earlier bound on the quantity of swindlers and does
not extend the message length by highly contrasted with
the disavowal of the same arrangement of backstabbers.
The fundamental upgrades of these strategies over before-
hand proposed techniques, when adapted to the stateless
scenario, are: (a) decreasing the message length to pay-
ing little respect to the coalition size while keeping up a
solitary decoding at the client's end (b) giving a consist-
tent combination between the renouncement and follow.
Hierarchical identity based encryption scheme proposed
in, built an identity based plans is one of the hotly debated
issues of current cryptography. In this paper, they propose
a mysterious various leveled character construct encryp-
tion plan based with respect to the q-ABDHE issue that is
completely secure in the standard model. The figure con-
tent size is free of the level of the progressive system. In
addition, the plan has short parameters, high productiv-
ity and a tight decrease. In depicted two new open key
show encryption frameworks for stateless recipients. Both
frameworks are completely secure against any number of
colluders. In their first development both figure writings
and private keys are of consistent size (just two gather-
ing components), for any subset of recipients. People in
general key size in this framework is direct in the aggre-
gate number of beneficiaries. The second framework is a
speculation of the first that gives an exchange off between
figure content size and open key size. To enhance security
and cryptography in wireless sensor systems, contended
that IBE is perfect for WSNs and the other way around.
The cooperative energy between the frameworks, depicted
how WSNs can exploit IBE, and presented results for
calculation of the Tate blending over asset obliged hubs.
In, proposed a unidirectional PRE accepting the arbi-
trary prophet. Notwithstanding, they demonstrated that
it is powerless against chosen cipher text assault (CCA).
At that point propose an effective unidirectional PRE
plan, for increasing high proficiency and CCA-security
utilizing the “token-controlled encryption” procedure,
under the computational Diffie-Hellman suspicion,
in the arbitrary prophet model and a casual however
sensible definition. In Issues of Identity-Based interme-
diary re-encryption addressed in, where cipher texts are
changed starting with one character then onto the next.
Their plans are good with current IBE organizations and
don't require any additional work from the IBE trusted-
party key generator. Likewise, they are non-intelligent
and one of them allows numerous re-encryptions. Their
security depends on a standard presumption (DBDH) in
the arbitrary prophet model.

In identity based encryp-
tion (IBE) and inner product encryption (IPE) plans
under the choice direct (DLIN) or symmetric outside
Di_e-Hellman (SXDH) suspicions are presented. In the
limited memory spillage demonstrate, their essential
plans achieve the most extreme conceivable spillage rate 1
O (1). In the consistent memory spillage model, variations
of the above plans appreciate spillage rate no less than 12
O (1). Among the outcomes, they enhanced the work of
in by exhibiting adaptively secure IBE plans. Cipher text
assaults for PRE plan is presented in. Their development
is productive Decisional Bilinear Di_e-Hellman supposi-
tion in the standard model. They likewise formally catch
CCA security for PRE plans by means of both a diver-
sion based definition and reenactment based definitions
that ensure generally compos able security. In presented
a more summed up idea of conditional proxy broadcast
re-encryption (CPBRE). A CPBRE plan permits sender to
produce a re-encryption key for some condition specified
amid the encryption, such that the re-encryption force
of the intermediary is confined to that condition as it
were. Cipher texts can be re-shown. This spares a consid-
erable measure of calculation and correspondence cost.
They propose a fundamental CPBRE plan secure against
picked plaintext assaults, and its augmentation which is
secure against replayable choose cipher text assaults
(RCCA). Both plans are unidirectional and demonstrated
secure in the standard model. To improve data security
three things to be considered are confidentiality, integ-
rity and availability. Major problems in cloud storage are
DNS attack and man in the middle attack.
encoder is implemented based on steganography method by using thermal images. They used both cryptography and steganography and has presented that their method provides more security for the hidden data and also improves performance.

2. System Model

As shown in the Figure 1 the information user and information proprietor ought to enroll to the cloud server. The cloud server produces primary & secondary key and access key for the enlisted users. On the off chance that the user needs to offer demand to the cloud for information, then the user ought to give access key for user verification. Cloud server creates shared key utilizing the primary and secondary keys of data user and data owner in order to avoid unauthorized sharing of data. On the off chance that the information proprietor intrigued to share the information, then he/she make and sends the mutual key to the information user who needs that information by means of email safely. The cloud server checks the mutual key and after that offer information to the requested user.

2.1 User Registration

In this module user going to make a user’s profile in this created application. For registering into the application the user should give their details like username, password, mobile number, mail id. By using this account the cloud user can directly interact with the cloud server.

2.2 Cloud Deployment

Cloud data service provider will contain the vast measure of information in cloud. For creating the account in the drop box first, should create a login in a drop box. Then user can create an application in a drop box. By using the developers console a user can create user own application.

2.3 Key Generation

In this module cloud server produces primary & secondary and access key for user validation, in the wake of enrolling into cloud. In the event that the client’s record (19) is hack by the other individual, then the unauthenticted individual can’t download any information from the cloud. Since the validate individual just knows the access key which is made in the user registration process. The shared key is created by utilizing the primary and secondary key of information user and information proprietor. In the event that the shared key is hacked by other information user, then he/she can’t get to the information by utilizing that shared key. Since every single information user having diverse shared key for getting to the information of a specific information proprietor. By utilizing access and shared keys, the entrance from unauthenticted and unauthorized client is diminished. Mutual key is utilized for removing the information from the cloud server. There might be opportunities to assault a record by a cloud proprietor itself. To avoiding that mutual key is utilized. The information proprietor makes that key and sends by means of email to the specific information user. Primary & secondary key and access keys are produced by utilizing random number generation method.

Syntax

```java
Random obj = new Random();
For() {
inrandomInt = obj.nextInt();
}
```

Shared key

- Data owner’s primary key : 2456378456
- Secondary key: 6758967248
- Data user’s primary key : 5134672412
- Secondary key : 3156782376

24675131 is the shared key for that particular data user.

2.4 Data Upload

Three methods are used in this module

- Encryption
- Steganography
- Merkle hash tree
In this module, the user given information is encrypted by utilizing AES calculation. The encrypted information is covered up into a picture called steganography. At that point the concealed picture is part into a few sections by utilizing merkle hash tree calculation and stores it into cloud.

2.5 Data Download

The information user can give the demand to the information proprietor. For looking the substance in the cloud global key word is utilized. While seeking the substance the information proprietor is additionally listed. In the wake of giving shared key to the cloud the cloud server is confirm the user and send demand to the information proprietor. In the event that the information proprietor is intrigued to share the information, then he/she make the mutual key and send it to information user by means of email. The mutual key is covered up into a picture. At that point the information user can download the picture and destegano it. By giving that mutual key to the cloud server then asked information is downloaded. The few sections of a pictures are totaled and destegano that aggregated picture. At that point the substance is deciphered by the cloud server, so the information user can see the original content.

3. Experimental Results

In the proposed scheme steganography is used. The time-span for encryption and decryption is shown in Figure 2. The encryption and decryption time is measured in terms of seconds. The time taken for both encryption and decryption is increased with increase in image size. The Figure 3 shows the time taken for encryption and decryption without MHT. The result proves that the proposed method is efficient and secure.

4. Conclusion and Future Work

In this paper, an encrypted file may still hide information using steganography, so data security is ensured. User confidentiality is improved by avoiding the mysterious access request to secretly advise in the cloud server about the clients’ entrance wishes. Data secrecy can be enhanced by wrapping up of exchanged values during transmission and hence the authentication can be achieved to guarantee data confidentiality and data integrity. In future the texture image can be used for steganography to achieving the more security.

5. References

1. Naor Dalit, Moni Naor, Jeff Lotspiech. Springer Berlin Heidelberg: Revocation and tracing schemes for stateless receivers. 2001 Aug; p. 41-62.
2. Ren Yanli, Dawu Gu. Efficient hierarchical identity based encryption scheme in the standard model. Wuhan University Journal of Natural Sciences. 2008 Dec; 13(6):665-69.
3. Boneh D, Gentry C, Waters B. Springer Berlin Heidelberg: Collusion resistant broadcast encryption with short cipher texts and private keys. 2005 Aug; p. 258-75.
4. Oliveira Leonardo B, Diego F Aranha, Eduardo Morais, Felipe Daguan, Julio Lopez, Ricardo Dahab. TinyTate: Identity-Based Encryption for Sensor Networks. International Association for Cryptologic Research. 2007 Jan; p. 1-10.
5. Chow SS, Weng J, Yang Y, Deng RH. Springer Berlin Heidelberg: Efficient unidirectional proxy re-encryption. 2010 May; p. 316-32.
6. Green M, Ateniese G. Springer Berlin Heidelberg: Identity-based proxy re-encryption. In Applied Cryptography and Network Security. 2007 Jun; p. 288-306.
7. Kurosawa Kaoru. Springer Berlin Heidelberg: Leakage Resilient IBE and IPE under the DLIN Assumption. 2013 Jun; p. 487-501.

8. Chosen-cipher text secure proxy re-encryption. Date Accessed: 23/10/2007: Available from: https://eprint.iacr.org/2007/171.pdf.

9. Chu CK, Weng J, Chow SS, Zhou J, Deng RH. Springer Berlin Heidelberg: Conditional proxy broadcast re-encryption. 2009 Jul; p. 327-42.

10. Beulah S, Ramesh Dhanaseelan F. Survey on Security Issues and Existing Solutions in Cloud Storage. Indian Journal of Science and Technology. 2016 Apr; 9(13):1-8.

11. Ananth SV, Sudhakar P. Performance analysis of a combined cryptographic and steganographic method over thermal images using barcode encoder. Indian Journal of Science and Technology. 2016 Feb; 9(7):1-5.