International Journal of Innovation Sciences and Research
Vol.7, No, 01, pp.1113-1116, January, 2018

Available online at
http://www.ijisr.com

RESEARCH ARTICLE

A Steganography based Framework to Forbid Insecure Practice in Cloud Platform

***Kannadasan, R., Vijayarajan, V., Manikandan, K. and Ezhilarasi, E.**

School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India

Accepted 15th December 2017; Published Online 31st January 2018

ABSTRACT

Latest technical developments in utility computing are necessary to permitted trivial and medium sized organizations to transfer their data's in the cloud, get profit from the groups, for example, auto-clambering and utility services. Already clouds can be extensively approved; there is an essential to report confidentiality anxieties of consumer information contract out to these areas. In this research work, we introduce a method for securing the privacy and reliability of customer information and reckoning from the insecure practice. For example, customers and also from the cloud-based platform organization manager himself. Finally, we prove a condition in what way the origin reliability and reality of IT technologies interactive program content managed by the cloud and it can be confirmed using steganography technique in a remote environment without illuminating the hiding information to the cloud manager.

Key words: Auto-scaling, Pay-as-you-go services, Steganography technique, Infrastructure-as-a-service.

INTRODUCTION

Now a day's world small and large administrations are using the cloud computing technique to secure their data's and also, they use cloud resources at what time they want. The Cloud Computing is a stimulating and satisfactory the innovative prototype it permits customers to contract out storing and computational assets on claim. Although cloud computing sources on recent method in place of virtualization and SOA, the main powerful features of this technology are progression in machine structural design, the obligation to practice and preserve the data's, and huge level bandwidth system frequencies. Furthermore, features are multitenancy; auto climbing and truncated budget also permit cloud to display effectively more than prototype and Grid. 33.25% in the IT enterprise defendants in a current cloud investigation and specified that they are previously using cloud facilities. Other 40% defendant companies are in a temporary period towards accepting cloud based facilities. All other professional area and technologies are also come into contact with the IT waves. Initially, the information is uploaded insecurely which has a danger of being hacked by the malicious persons. Furthermore, the data kept at remote servers is under the observation of unknown persons who can do something with our information. At present time, I Cloud can be frolicked the part of a corruption, helping to path depressed by the iPhone of a customer it was taken on a journey craft. It can be performed in the cloud platform. For instance, cloud platform exists in the last stage; it agrees the progress of provable confidence resolutions and at that moment layers in the software cache on topmost location.

Corresponding author: **Kannadasan, R.,**
School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India.

System Design

The administrator distribute task to all teams. So, the admin selects one image and important task information hide with image using the encoding algorithm. The data can be stored in to the cloud platform. Team member gets the administrator sending image and then member click that image and decodes the admin sending task information using the Decoding Algorithm. Team member make task report based on succeed sending task details and then hiding the finished task with image using encoding algorithm. Administrator gets team members sending task report and takes the hiding image by decoding algorithm.

Literature review

They proposed a method called novel WEE system for encrypting a condition over Zp. The system has the pleasant ET-property over the Zp. Built on our WEE system and also, they proposed five confidentiality protective and well-organized outsourcing procedures for the GE (Gaussian-Jordan elimination), GJE, matrix element, linear scheme solver, and matrix transposal. The linear scheme solver and matrix transposal procedures have cheating resistant machinery. The experimental outcomes display that the procedures have important proficiency gain for a customer (Chen *et al.,* 2015). In this paper, they drew the present position of the requirement procedure for the Java API in the Trustworthy Computing. It develops in present Java archives for TC by provided that streamlined entrance to the huge position in TC purposes whereas uphold theoretical reliability and observing in the conditions (Toegl *et al.,* 2009). They sharing the key built on the source of active information re-encryption is put on to a cloud computing method in a exclusive way to report the anxieties of a mobile device background, as well as restrictions on customer wireless data practice, storing measurements,

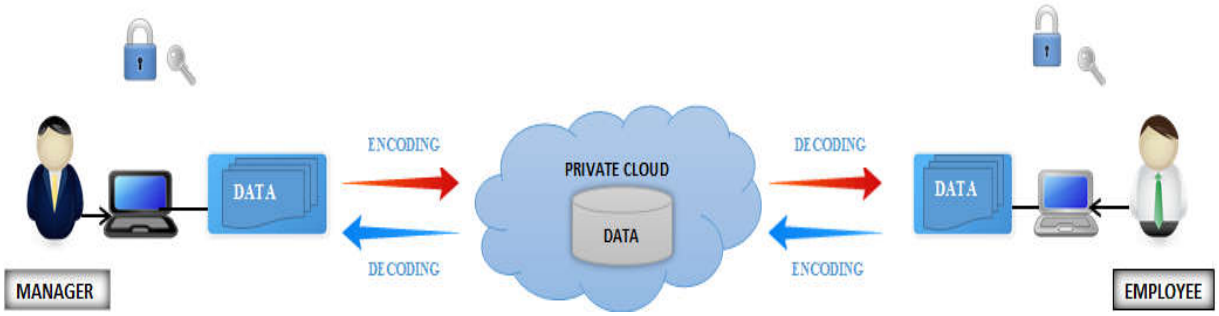

Figure 1. Architecture of the system

managed power, and the battery life. A versioning olden time's mechanism successfully manages keys for always altering user population. To conclude, a proposal on profit-making mobile and cloud platforms can be authorize the presentation of the model (Tysowski *et al.,* 2011). This paper results on the growth and formal guarantee (evidence of semantic protection) of a compiler from a C minor (a C like authoritative language) by the Coq evidence supporter for user interface design and for verifying its accuracy. The specialized compiler is valuable in setting of proper approaches useful to authorization of precarious software: authorization of the executed promises that security assets verified in the program embrace for the implemented collected code as fine (Leroy, 2009). They present a different mechanism for cheering belief in a cloud atmosphere known TVEM. This method used to explain the essential safety task of cloud by allowing revelries to launch belief interactions wherever a material vendor generates and goes a simulated location in a platform possessed by the distinct provision supplier. This paper demonstrates the requirements, plan, and structural design to that approach (Krautheim *et al.,* 2010). In this paper, they create form based on the current proposal for measuring integrity of computations executed by theoretically untrusted providers presenting some optimizations, thus restrictive in the clouds to be funded for integrity assurances, and making it appropriate to many situations (Di Vimercati *et al.,* 2013).

The writers' proposal can be supreme proficiency and knowledge as they converse the enormously stimulating topics of information ownership, privacy securities, data flexibility, quality of service and service levels, bandwidth costs, information protection and maintenance. As the most present and broad guide to serving you catch your way complete a maze of protecting minefields, this volume is compulsory reading if you are tangled in any characteristic of the cloud computing (Virtualization, 2005). They suggested a technique wherever data is encoded by the image as key and to create this key from the image and them charity variance development procedure for multi-level subdivision. Outcomes are related with the other nature stimulated algorithms (Sahu and Bhadoria). It is certainly that cloud computing can demonstrate to be a boon in the today's work situation hence this paper contracts with data confidence concerns connected to the cloud computing so that the data centers can offer a good atmosphere to preserve the data safe (Biswas, 2014). They proposed Xoar, a adapted version of Xen that retrofits the modularity and separation moralities used in the microkernels onto a complete virtualization policy. Xoar disruptions of the regulator VM into the single-purpose mechanisms called the provision VMs (Colp *et al.,* 2011).

Steganography technique

Steganography is the technique of hiding private or delicate information within somewhat that seems to be nothing out of the normal. It is successful to improve its status owing to the advocate progress and secret information of computer handlers in the network. It is well-defined as the learning of imperceptible message that frequently compacts to the methods of walloping the presence of transferred data. In general, data inserting is realized in message can be image, audio-visual aid and other dedications. The top-secret message is attained to insert a data in to the image and make a steganography image.

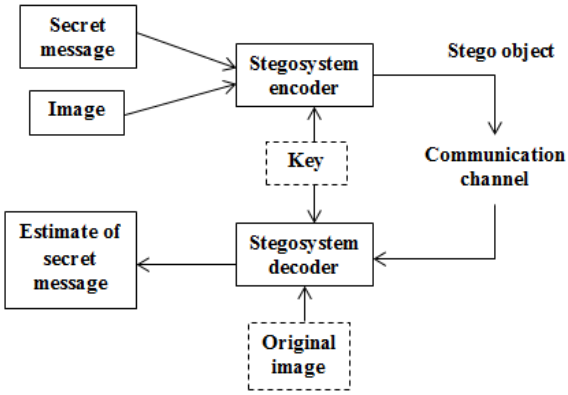

Figure 2. Steganography basic model

In general, steganography is well-known as "imperceptible" message. It means to hide the messages existence into the medium (audio, video, and image). Now a day's steganography scheme using interactive program entities are image, audio, video. It covers mass media for the reason that persons frequently convey images over the email or shared by the net. It can be dissimilar from protective the authentic of a dispatch. It simply says, hides data in to the image.

Proposed method

The proposed method for cloud security is a new method, where we are using image as encryption key to encode the data or information. The image can be removed by decryption key to decrypt the data which can be hidden in the image. Our proposed method is using security procedure to uphold the secrecy, privacy and exactness of the data. The inclusive procedure of the technique can be stepped out:

Point 1: The data can be stored in to the cloud platform.

Point 2: Select any image, and put in to procedure. Hiding data using the image.
Point 3: The encoding key has been created by using an image.
Point 4: Encoding can be method using to create access key.
Point 5: The image can be removed by the decryption key.
Point 6: Now the decryption will be process using the secret key.

A. Encryption

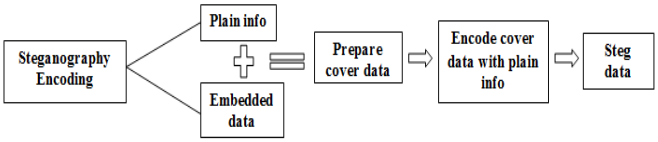

Figure 3: Steganography encryption technique

The Steganography encryption method is adding a small design as a layer completed in an image. Sometimes the design is obscure although at other times but it looks like a little bit of film ounce. The design is what encrypts the real message and enhances it in to the image. The steganography encoding is the technique to combine both theplain information and embedded data and it can be prepared to cover data and encode cover data with plain information and finally it can be a steg data.

Table 1. Encryption algorithm

```
Begin
Key key = Publickey.generateKey ();
Cipher c = Cipher.getInstance("AES");
c.init(Cipher.ENCRYPT_MODE, key);
Byte [] encVal = c.doFinal (Data.getBytes ());
EncryptedValue = new BASE64Encoder ().encode (encVal);
return encryptedValue;
End
```

B. Decryption

Figure 4. Decryption technique

To decode the message which is encoded by the image and using the similar encryption procedure to get the stego image. And then remove the inserted message using the same steganography procedure. The steganography decoding is the method to decode the plain information which is encoded in the images and using the access key to decode the covered data and then removing the covered data and get that information.

Table 2: Decryption algorithm

Steganography Classifications

Normally steganography is characterized in to the resultant features and chart displays the top steganography procedures.

- **High Dimensions**: Extreme dimension of data is inserted in to the image.
- **Invisibility**: The data which is covered by the image can invisible to the users.
- **Robustness**: Inserting information can be complete if image drives to the certain alteration are collecting, climbing, riddling and noise.
- **Temper Resistance**: hard to modify the information when it can be inserted in to image.
- **Computation Complexity**: It can be difficultly computed to insert and remove the image**.**

Table 3. Steganography measures

Methods	Benefit	drawback
High Dimensions	High	Low
Invisibility	High	Low
Robustness	High	Low
Temper Resistance	High	Low
Computation Complexity	Low	High

Experimental result

Steganography is the technique of hiding private or delicate information within somewhat that seems to be nothing out of the normal. Now a days steganography schemes used various interactive program entities are images, audios and video. It covers mass media for the reason that persons frequently convey images over the email or sharing by network. It can be dissimilar from protective the authentic of a dispatch. It simply says, hides data in to the image. Hiding the data with audio and video is not good than using image. Because it takes lot of time to encrypt and decrypt the messages. Using the image to hide the information is better than audio and video.

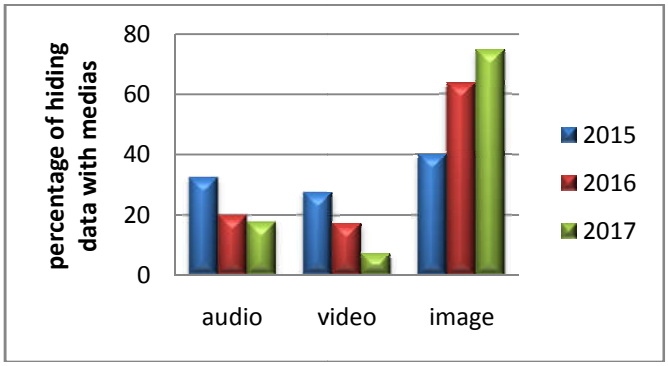

Figure 4. Comparison between different steganography methods

Merits and Demerits

a) It can be used in the method of hiding not the data but password to stretch that information. It is hard to detect but receiver can be detect.
b) It can be applied in to the different format in digital image, audio and video file. It is faster compared with the large number of software's.
c) It offers better confidence for sharing data in to the LAN, MAN and WAN.
d) The privacy of information id preserved by the procedures, and if the procedures are known then it's all completed.
e) If this method is gone to the wrong persons like hackers, terrorist and criminals and then it can be very much risky for all.

Conclusion

Steganography is the recently developed technique as well as a very elaborated method of hiding the information in today's situation where the cloud is frequently used by the all users and their data keep coordinated in to the cloud at every time. In this paper, cloud computing can be knowledgeable in highly development proportions and is presenting in the excessive scenarios. It is the leading tasks to extensive implementation of cloud facilities are consumer privacy and reliability anxieties. At last, we offered and properly proved a real-world result to report this difficult and this protocol is used for performing complex computations in the cloud environment is displayed.

REFERENCES

Chen, Y. R., Shen, S. T. and Tzeng, W. G. 2015. Weave ElGamal Encryption for Secure Outsourcing Algebraic Computations over Zp. *IACR Cryptology ePrint Archive*, *2015*, 947.

Tysowski, P. K. and Hasan, M. A. 2011. Re-Encryption-Based Key Management Towards Secure and Scalable Mobile Applications in Clouds. *IACR Cryptology EPrint Archive*, *2011*, 668.

Leroy, X. 2009. A formally verified compiler back-end. *Journal of Automated Reasoning*, *43*(4), 363-446.

Krautheim, F. J., Phatak, D. S. and Sherman, A. T. 2010. Introducing the trusted virtual environment module: a new mechanism for rooting trust in cloud computing. In *International Conference on Trust and Trustworthy Computing* (pp. 211-227). Springer Berlin Heidelberg.

Di Vimercati, S. D. C., Foresti, S., Jajodia, S., Paraboschi, S. and Samarati, P. 2013. Integrity for join queries in the cloud. *IEEE Transactions on Cloud Computing*, *1*(2), 187-200.

Virtualization, A. 2005. Secure virtual machine architecture reference manual. *AMD Publication*, (33047).

Sahu, S. and Bhadoria, A. Survey on Cloud computing security using steganography.

Biswas, K. 2014. Ensuring Data Security in Cloud Computing Using encryption. *International Journal of Computer (IJC)*, *8*(1).

Colp, P., Nanavati, M., Zhu, J., Aiello, W., Coker, G., Deegan, T. and Warfield, A. 2011. Breaking up is hard to do: security and functionality in a commodity hypervisor. In *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles* (pp. 189-202). ACM.

Toegl, R., Winkler, T., Nauman, M. and Hong, T. 2009 November). Towards platform-independent trusted computing. In *Proceedings of the 2009 ACM workshop on Scalable trusted computing* (pp. 61-66). ACM.

****