International Journal for Research in Engineering Application & Management (IJREAM)
Special Issue – ICRTET-2018 ISSN : 2454-9150

Securing information on Cloud platform using Steganography

Dipesh R. Agrawal
Assistant Professor
Department of Computer Engineering,
SNJB's Late Sau. Kantabai Bhavarlalaji Jain College of Engineering, Chandwad, India

Abstract

As, security is the biggest issue for the information which is stored or shared on cloud, because of heterogeneous – networks, hardware platforms, operating systems and user interfaces, used by end users and provided by service providers. Cloud computing works on different services and interactions between them, based on certain constraints between different stakeholders, as per need. The information which is to be stored or shared on the cloud can be made secured by using the steganography technique which hides the secret information into another raw data while storing on cloud or sharing through heterogeneous networks or platforms

This paper illustrates basic steganography techniques that can be organized using a service oriented paradigm, which is popularly known as a new generation distributed computing platform. Paper describes how steganography techniques can be used with distributed environment using cloud computing and service oriented architecture. SOA is a mechanism to develop platform independent, reusable and autonomous blocks of functionalities, called services.

***Key Words — Cloud Computing, Service Oriented Architecture (SOA),Steganalysis, Steganography*.**

Introduction

As technology is growing, there is a rapid increase in use of computers by individuals. This result in large information sharing through networks among various devices like Laptops, Mobiles, Smart phones and other handheld devices. This communication among the devices having heterogeneous hardware and software platforms requires two things. One is a robust software environment which can work on existing network infrastructure and can support heterogeneous software platforms of various devices. Like – Distributed Computing, Service Oriented Architecture and Cloud Computing. Second is, a secure way of communication which can keep users data secure from intruders while it is transmitted through a network. Like – Cryptography, Network Security, Steganography[1].

Cloud Computing is the advanced version of distributed computing, to provide seamless user interfaces to the user even though the user is working on different shared resources. Cloud computing is based on three models – IaaS (Information as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service). Cloud computing provide different deployment models – Public Cloud, Private Cloud, Community Cloud and Hybrid Cloud, based on their use and architecture. Cloud computing has following features - On demand self-service. Pay-per-use billing, Broad network access, Resource pooling, Rapid elasticity, Measured Service, virtualization, Multi tenancy, Service level agreement (SLA), Heterogeneity [2].

RELATED WORK

To provide security over such heterogeneous platform, we have two information hiding mechanisms with us, Cryptography & Steganography. In cryptography, at sender side, an original message (plain text) is encrypted (scrambled) using any encryption algorithm along with some special keys and converted into an encrypted message (cipher text). this cipher text is decrypted at receiver side using relevant decryption algorithm along with some keys that are provided with receiver[4]. Another mechanism, steganography, refers to hiding information by embedding within unremarkable cover media. So, if intruder gets the message, it can see only the cover media and not the original message. Various steganography algorithms are proposed for different kinds of media and for different kinds of accuracies.

The paper describes how various steganography techniques for different media and some steganalysis methods that can be used with a new generation distributed computing environment – Cloud Computing.

PROPOSED WORK

An online, cloud based - service oriented steganography environment (interface) is described here.For this, web service mechanism is used to develop basic unit called Services, to communicate over the network in a heterogeneous platforms.

STEGANOGRAPHY

Steganography can be used with various media like – Text, Images, Audio and Video. There are various techniques for each media.

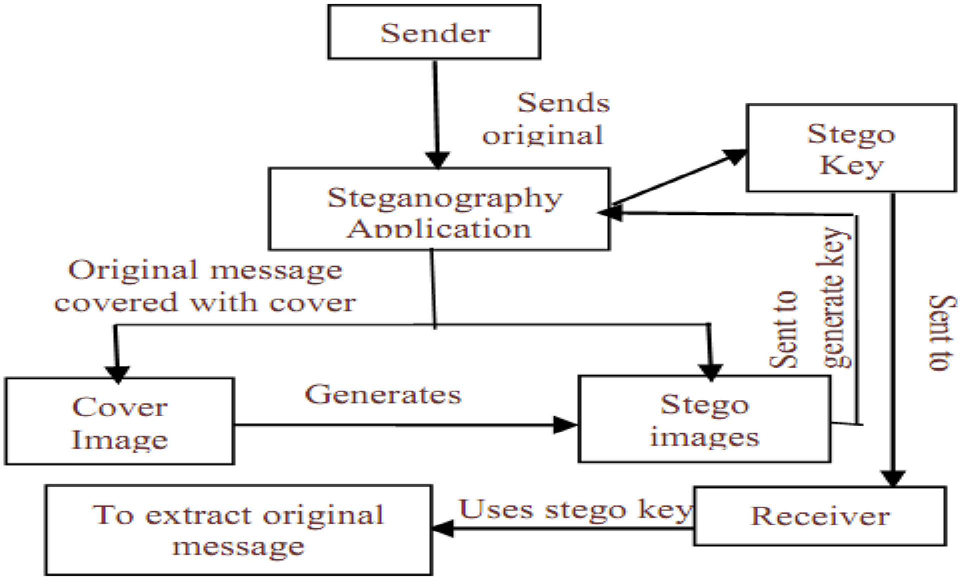

Fig. 1. Architecture of Steganography

For text steganography – A secret message can be hidden in a formatted text cover for ex. SMS texting [5].

For image steganography – LSB (Least Significant Bit) [3], Masking and Filtering methods can be used.

For audio steganography – techniques like Low Bit Coding (LBC) [4], Bit Modification Technique [8] can be used.

For video steganography – Least Significant Bit (LSB), data can be hidden into video streams [9].

For each type of steganography algorithm, a service can be defined and registered on the cloud. So that the intended user

Customer can search, identify and use these services, for applying with users information which is to be made secure.

All these services are presented to the user in the form of a dashboard like structure/interface. From this dashboard, user has to select a particular steganography algorithm and has to apply to the information.

STEGANALYSIS [10]

It is a technique of detecting secret messages embedded in original information. There are two types of steganalysis – Blind Steganalysis and Targeted Steganalysis.In blind steganalysis, an algorithm which is used for steganalysis can detect all forms of steganography.Some techniques used for blind steganalysis are: Blind steganalysis of JPEG image using calibration and Blind Steganalysis in Spatial Domain.In Targeted Analysis, algorithm which is used for steganalysis can detect some specific forms of steganography.Techniques used for this are – LSB Embedding and the Histogram Attack, Simple Pair Analysis

Steganalysis technique can be used digital forensics or cyber forensics to identify hidden information in stego text/images/audio or video.

IMPLEMENTATION VIEW

Above mentioned techniques of Steganography and Steganalysis can be implemented using service oriented environment using various tools like – Microsoft's Visual Studio 2008, Sun Microsystems's J2EE platform etc. Basic building blocks of SOA are – Web

Services, Web Services Description Language (WSDL), simple Object Access Protocol (SOAP), Universal Description Discovery & Integration (UDDI), Extensible Markup Language (XML) etc [10]. These components helps to develop a platform independent environment required for various web services to communicate with each other. SOA can be treated as a new generation distributed computing environment and it can feature all the characteristics of distributed computing; like- transparency, mobility, availability, heterogeneity,scalability, reusability and so on.

To have this Service Oriented view of above steganography techniques, we will have to consider following steps [11].

Define services for secret messages (i.e. for stego) – in this step, we can define each secret message as an independent service. So that these messages can be embedded with cover.

Define services for cover – in this step; we can define an independent service for each cover types. Using these covers, we can hide secret information.

Define service for stego – in this step, it is decided that, to hide the important information, which type of (text, image, audi, video) raw data can be used.

Define service for storage – in this step; we can define services to store secret message and cover.

Define services for steganography algorithms – in this step; we can define services which can include algorithmic steps for each steganography technique.

Define services for steganalysis algorithms – in this step; we can define services to detect secret messages from available information.

Define Service Level Agreements (SLAs) – SLAs [3] are defined to express the terms and condition which should be followed by the service provider and service user. Like – billing constrains, duration, etc.

CONCLUSION

The proposed system provides us a new generation platform independent information security approach in cloud computing environment using steganography and steganalysis techniques, for various media. We can hide secret messages using various steganography algorithms and techniques andwe can detect the secret messages back from the availableinformation, using various algorithms and techniques. Wecan break all these things in the form of independentservices, that can communicate with each other in anorganized way, using service level agreements, to generate a customized applicationaccording to users need, by collecting or including the required services inan application

REFERENCES

[1] **Dipesh Agrawal**, Steganography &Steganalysis Using Service Oriented Architecture1st International Conference on Recent Trends in Engineering & Technology, Mar-2012 Special Issue of International Journal of electronics, Communication & Soft Computing Science & Engineering, ISSN: 2277-9477

[2] **Saju Mathew , Dr. T. Anuradha**,Security For Cloud Computing UsingSteganography, International Journal of Computer Engineering and Applications, Volume XI, Issue VI, June 17, www.ijcea.com ISSN 2321-3469

[3] **Ataussamad, Prakash Shiva**, A Review in Cloud Computing Security Using Steganography, International Journal of Advance research, Ideas and Innovations in Technolog,ISSN: 2454-132X, (Volume2, Issue6)

[4] **PiyushMarwaha and PreshMarwaha**, "*Visual CryptographicSteganography in Images"*, 2nd International Conference onComputing Communication and Networking Technologies 29-31 July, 2010.

[5]Mohammad Shirali-Shahreza, “*Steganography in MMS”,*Multitopic Conference, 2007, INMIC 2007, *IEEE International*.

[6]Ming, ZangRu, NiuXinXin, Yang Yixian, “Analysis of Current Steganographic Tools: Classifications and Features”, Proceedings of the 2006 International Confrerence on Intelligent Information Hiding and Multimedia Signal Processing.

[7]Masahiro Wakiyama, Yasunobu Hidaka, Koichi Nazaki, “An audio Steganography by a low-bit Coding Method with WAVE Files”, Sixth International Conference on Information Hiding and Multimedia Signal Processing, 2010.

[8] KaliappanGopalan, Qidong Shi, “Audio Steganography Using Bit Modification – A Tradeoff on Perceptibility and Data Robustness for Large Payload Audio Embedding”, Computer Communications and Networks (ICCCN), 2-5 Aug. 2010.

[9]Daniela Stanescu, “Embedding Data in video Stream Using Steganography”, Applied Computation Intelligence and Informatics,2007. SACI 2007, 4th International Symposium on, 27-28 May 2007.

[10]SandroGeric, NevenVrcek, “Prerequisites for Successful Implementation of Service Oriented Architecture, Proceedings of the ITI 2009, 31st International Conference on Information Technologies Interfaces, June 22-25, 2009Cavtat, Croatia.

[11]PooiaLalbakhsh, SepidehRavanbakhsh, “Service Oriented Steganography*”, International Conference on Signal ProcessingSystems 2009”.*