Epitome Journals
International Journal of Multidisciplinary Research

A Solution to Cloud Security : Image Steganography

Aparna G. Korde,
Department of Computer Science,
Poona College, University of Pune, Pune, India
Email : apkorde@gmail.com

Abstract :

The paper focuses on characterization of information hiding possibilities in Cloud Computing. After general introduction to cloud computing and its security, we move to brief description of steganography. In particular, we introduce classification of steganographic communication scenarios in cloud computing which is based on different techniques of steganography. These techniques and applications must be taken into account when designing secure cloud computing services.

Keywords : *Cloud computing, Steganography, stego-image, Masking, Filtering, Feature tagging, spatial domain, transform domain, distortion technique, digital watermark.*

RESEARCH PAPER :

INTRODUCTION :

Steganography is ‘covered writing’. The main purpose of steganography is to hide the fact of communication. In this, the sender embedded its message into the text, image, video, or audio file so that hackers will not be aware of the message. Section II considers the basic definition and different types of deployment and service models of cloud computing and list of the threats (of our concern), regarding security in implementing the cloud. Section III focuses on the solution to these threats as ‘Steganography’, its classification, types. Section IV has the different types of steganography techniques that can be implemented for our cloud service. The next section V gives details of applications of these techniques. Future work is stated by section VI. The complete work is summarized by conclusion in section VII. In addition, all related work is used by this paper is mentioned by section VIII.

CLOUD COMPUTING (CC)

CC is a pay-per-use model for enabling available, convenient, on demand network access to a shared pool of configurable computing resources like networks,servers, storage, applications, services etc., that can be rapidly provisioned and released with minimal management effort or service provider interaction. Key characteristics of cloud computing includes: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

Deployment Models of Cloud :

Public Cloud : A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space.

Private Cloud : A private cloud is established for a specific group or organization and limits access to just that group.

Community Cloud : A community cloud is shared among two or more organizations that have similar cloud requirements.

Hybrid Cloud : A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community [3].

Service Models provided by Cloud:-

Software-as-a-service (SaaS) : This model allows the consumer to use provider’s applications running on a cloud infrastructure. Applications can be accessed from various client devices through a thin client interface such as web-based e-mail. It hides the complexities from end users. The consumer does not manage or control underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform-as-a-Service (PaaS) : This model allows the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Infrastructure-as-a-Service (IaaS) : This model allows the consumer to obtain processing, storage, networks, and other fundamental computing resources and be able to deploy and run a range of software. The consumer does not manage or control the underlying cloud infrastructure but controls operating systems, storage and deployed applications and may have limited control of select networking components.

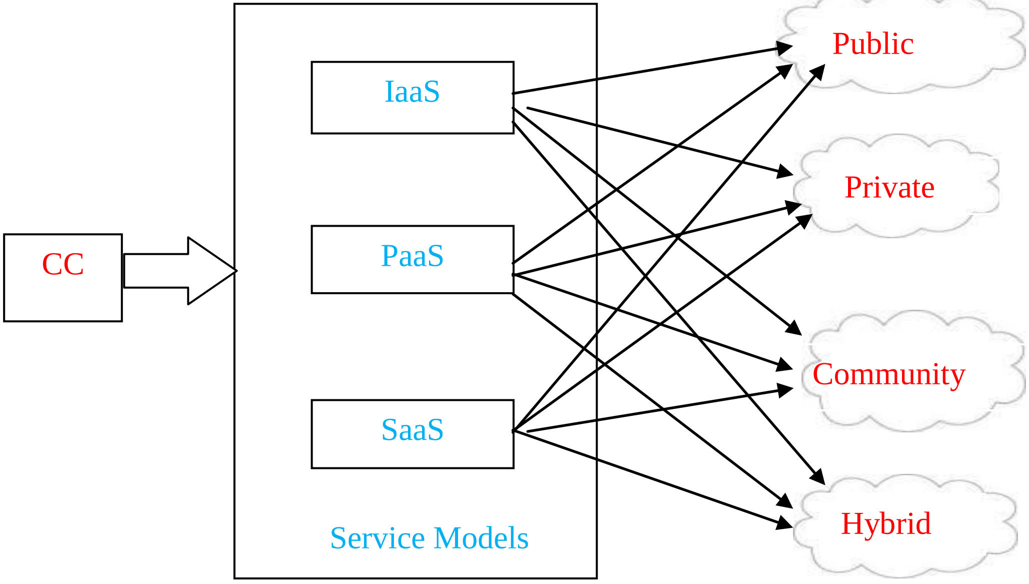

Fig 1: Models in cloud computing

Cloud security threats :

Cloud Security Alliance defined seven most important threats for cloud computing, mainly, [4]

Threat #1: Abuse and Nefarious Use of Cloud Computing (different "activities" e.g. spamming, Malware code, passwords cracking, DDoS attacks, botnet C&C etc.),

Threat #2: Malicious Insiders,

Threat #3: Data Loss or Leakage,

Threat #4: Account or Service Hijacking,

Threat #5: Insecure Interfaces and APIs.

Threat #6: Shared Technology Issues – many underlying components of cloud computing services were not designed to offer strong isolation for multi-tenancy. Attackers focus on the operations of othercloud customers, and how to gain unauthorized access to their data,

Threat #7: Unknown Risk Profile – ambiguous information about with who you will be sharing yourinfrastructure, in addition to logging data e.g. network intrusion logs, redirection attempts and/or successes etc.

INFORMATION HIDING

Steganography is a technique to hide the information in digital media. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media; audio, video, and images [1]. Therefore, the confidentiality and data integrity are required to protect it against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding. The host data is corrupted but hidden data in invisible when an unauthorized person analysis those data. The Steganography goal is that securely communication channel is completely unpredictable.

Some terms used in steganography are: [5]

Cover Image : The medium in which information is to be hidden. It may be an audio, video, image or a text file.

Stego-image : A medium within which information is hidden.

Message : The data to be hidden or to be extracted.

Stego-key : It's a secret value which helps in encoding or extraction of data, without which data cannot be encoded and extracted. Steganography technique is classified as: [2]

Technical Steganography

Linguistic Steganography

Technical Steganography

In this technique, we use invisible ink or microdots and other sizes reduction methods. This is a scientific method to hide data .Technical Steganography is used in the following technique :

Video Steganography : In this technique, we can easily hide large data video file. Video file is generally a collection of images and sounds. Any small but otherwise noticeable distortion might go by unobserved by humans because of the continuous flow of information.

Audio Steganography : In this technique, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio steganography software can embed messages in WAV, AU and even MP3 sound files.

Text Steganography : In text steganography the message is hidden in the text and we use the different methods to hide the message in text by changing the last bit of message. Sometimes, one sentence in ten times and use of blank space in alphabet terms is used.

Image Steganography : In this technique, hide information; straight message insertion may encode every bit of information in the image. The messages may also be scattered throughout the images. A number of ways exist to hide information in digital media.

Protocol Steganography : In this technique, steganography can be used in the layer of OSI network model and cover channels protocols. Steganography is referred to the technique of embedding information within messages and network control protocol used in network transmission. The information is adding in TCP/IP header and sends in the network.

Linguistic Steganography:

This technique hides the message within the carrier in some non-obvious ways. It is categorized into two ways :

Semagrams : Semagrams use some symbols and signs to hide the information. It is further categorized into two ways:

Visual Semagrams : A visual semagram uses innocent-looking or everyday physical objects to convey a message, such as doodles or the positioning of the items on a website.

Text Semagrams : This hides a message by modifying the appearance of the carrier text, such as subtle changes in font size or type, adding extra space, or different flourished in letters or handwritten text

Open Code : This hides a message within a legitimate carrier message in the ways that are not obvious to an unsuspecting observer.

Jargon : This is one type of language which is meaningless to other but can be understood by group of people. Only Jargon codes include symbols used to indicate the presence and type of wireless network signal, underground terminology, or an innocent conversation that conveys special meaning because of the facts that are known to the speakers only. A subset of jargon codes are cue codes, where certain pre-arranged phrases convey meaning.

Covered Cipher : Covered or concealed ciphers hide a message openly in the carrier medium so that it can be recovered by anyone who knows the secret for how it was concealed.

Null Cipher : A null cipher hides the message according to some prearranged set of rules, such as "read every fifth word" or "look at the third character in every word."

Grille Cipher : A grille cipher employs a template that is used to cover the carrier message; the words that appear in the openings of the template are the hidden message.

STEGANOGRAPHY TECHNIQUES

Spatial Domain Method : There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are unpredictable to human eyes.

Transform Domain Technique : This is a more complex way of hiding information in an image. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Most of the strong stenographic systems today operate within the transform domain. The advantage of this technique over spatial domain techniques is that they hide information in areas of the image that are less exposed to compression, cropping, and image processing. All transform domain techniques are not dependent on the image format and they may run on lossless and lossy format conversion.

Distortion Technique : In this technique the decoding process is based on the decoding function. The decoding function checks difference between original cover image and the distorted cover image to restore the secret message. In this, a stego-image is created by applying sequence of modification to cover image. The message is encoded at some random chosen pixels. If the stego image is different from cover image at the given message pixel, the message bit is "1". Otherwise, message bit is "0".

Masking and Filtering : These techniques hide information by marking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding it into the noise level. The hidden message is integral to the cover image. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image. Advantages of Masking and filtering Techniques: This method is much more robust than LSB replacement with respect to compression as information is hidden in visible part of the image.[5]

APPLICATION OF STEGANOGRAPHY

Copyright Protection : A secret copyright notice can be embedded inside an image to identify it as intellectual property. In addition, when an image is sold or distributed an identification of the recipient and time stamp can be embedded to identify potential pirates. A watermark can also serve to detect whether the image has been subsequently modified.

Feature Tagging : Captions, annotations, time stamps, and other descriptive elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features. [7]

Secret Communications : In many situations, transmitting a cryptographic message draws unwanted attention. The use of cryptographic technology may be restricted or forbidden by law. However, the use of stenography does not advertise covert communication and therefore avoids scrutiny of the sender, message and recipient. A trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers or eavesdroppers.

Digital Watermark : A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal.

Use by terrorists : Steganography on a large scale used by terrorists, who hide their secret messages in innocent, cover sources to spread terrorism across the country. It comes in concern that terrorists using steganography when the two articles titled "Terrorist instructions hidden online" and "Terror groups hide behind Web encryption" were published in newspaper[5].

FUTURE WORK

It is now convenient for people to transmit mass data in the form of text, images, audio and video through cloud computing. However, there is always a threat from the hackers of stealing the valuable information. The organizations such as banking, commerce, diplomacy and medicine, private communications are essential. The research is to device strong stenographic and steganalysis technique is a continuous process. With proper usage, Steganography can prove to be the ultimate solution to information hiding.On the contrary; its misuse is devastating and unthinkable.

In order to minimize the potential threat of malicious use of steganography to public security effective steganalysis (detection) methods are needed. This requires in-depth understanding of the functionality of particular cloud service and the ways it can be used to enable hidden communication. Considering however, variety and complexity of the cloud computing services there is not much hope that a universal and effective steganalysis method can be developed.

CONCLUSION

Cloud is a fantastic enabler when it comes to resource centralization and allows remote resources to come together under one environment and data becomes correspondingly "denser." While this is a boon for management, it can become challenging from a security standpoint, particularly when considering tools that operate across that data in aggregate. Studies say that digital image steganography is very useful as a powerful tool for cloud service providers.

REFERENCES :

[1] B. Pfitzmann, “Information Hiding Terminology,” Proc. First Int’l Workshop Information Hiding, Lecture Notes in Computer Science No. 1,174, Springer-Verlag, Berlin, 1996, pp. 347-356.

[2] DIGITAL IMAGE STEGANALYSIS FORCOMPUTER FORENSIC INVESTIGATION Nanhay Singh, Bhoopesh Singh Bhati, R. S. Raw Ambedkar Institute of Advanced Communication Technologies and Research, Delhi, India.

[3] The Basics of Cloud Computing Alexa Huth and James Cebula.

[4] Is Cloud Computing Steganography-proof?Wojciech Mazurczyk, Krzyszt of Szczypiorski

Institute of Telecommunications Warsaw University of Technology Warsaw, Polan.

[5] Volume 4, Issue 5, May 2014 ISSN: 2277 28X International Journal of Advanced Research in Computer Science and Software Engineering

[6] Detection of Double-Compression in JPEG Images for Applications in Steganography Pevny, T. ; Dept. of Comput. Sci., Binghamton Univ., Binghamton, NY ; Fridrich, J.

[7] IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.4, April 2007Hiding Encrypted Message in the Features of ImagesKh. Manglem Singh, S. Birendra Singh and L. Shyam Sundar Singh DOEACC Centre, Imphal – 795001, India