Detection of Steganographic Intrusion in Cloud

J. Anitha Ruth
Asst. Professor (SrG)
MCA Department
SRM University

A. Meenakshi
Asst. Professor (Sr G)
MCA Department
SRM University

H. Srimathi, Ph.D.
Professor
SRM University

ABSTRACT
The customer's try to migrate the data from desktop to cloud.. The data stored in cloud is targeted by potential threat. A potential threat is caused due to malicious hacker attack or data leakage in cloud. These threats in cloud environment arises the need for providing secure and safe information security system that can protect the data that is outsourced. In this paper we propose a framework for Intrusion Detection (ID) which identifies steganographic intrusion in cloud.

General Terms
Security, Intrusion detection system

Keywords
Cloud Storage, Steganographic intrusion, IDS.

1. INTRODUCTION
National Institute of Standards and Technology (NIST) defines cloud computing [1] as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources.(e. g) networks, servers, storage, applications and services. The key challenge to cloud computing is to ensure the safety of the data that is stored in cloud. The cloud computing infrastructure which is of multitenant architecture is exposed to several threats, such as cross site scripting vulnerabilities, database attacks like SQL injection attacks, operating system attacks like machine code injection, data leakage due to data deduplication in cloud storage services and malicious data that is transferred through covert channel communication. These threats affect the integrity, confidentiality of the data stored in cloud. To overcome these threats there are encryption methods to save guard the data that is outsourced. Encryption[2] of data protects the confidentiality of the data. But does not guaranteethat it will not be affected by potential threats such as insider attack or covert channel communication.. Hence there needs an effective mechanism to keep confidentiality of data secure and to avoid illegal access on the data stored in cloud. To handle this problem effectively there needs an intrusion detection system to monitor, analyze and detect the intrusion that affects the data in cloud storage.

The Cloud Security Alliance [3] reports Top security threats that the cloud computing environment is exposed to.

- Abuse and Nefarious use of cloud computing
- Insecure Application programming Interface
- Malicious Insiders
- Shared Technology Vulnerabilities
- Data loss/leakage
- Account/Service and Traffic Hijacking

From the above mentioned threats this paper focuses on the threat due to data leakage[4] that occurs when the data is transferred to cloud through hidden communication Steganographic communication is considered as hidden communication which can transmit malicious data into the cloud storage .

The paper is organized as follows section 2 provides an overview of how steganographic intrusions affect the cloud storage. Section 3 deals with the related work on steganographic attacks on data stored in cloud. Section 4 represents a framework for the proposed IDS for detecting the steganographic intrusions in the cloud. Finally we conclude the paper and present directions for future work in section 5.

2. STEGANOGRAPHIC INTRUSION IN CLOUD STORAGE

2.1 Definition of Steganography
Steganography[5] refers to a process of concealing secret data in various forms of digital media such as text,image ,audio or video. For instance, If a digital image is utilised as a medium it is consequently known as a cover-image whereas the altered image after the concealing process is called as stego-image.

Steganographic method ensures security to the data stored in the cloud by means of hiding the confidential data through images, video and audio. But certain situations the steganographicmethod act as an medium for intrusion. The intrusion can be done by exploiting the secrete data which is hidden in the stego-image(ie) altered image or text.The simplest method is the intruder can attack the stego-image by replacing the Least significant bit (LSB) bit of the image. Hence the confidentiality of the data stored in the stego-image is lost.

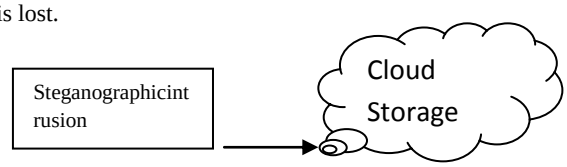

Fig 1Steganographic intrusion in Cloud Storage

2.2 Methods used in Intrusion Detection
An intrusion[6] is any set of actions that endeavour to compromise the integrity, confidentiality or availability of a data. The intrusion can be detected by two methods

- Misuse detection or Signature based intrusion detection
- Anomaly detection.

The Signature based intrusion detection [7] defines patterns or set of rules that are stored in the database to decide whether the pattern is a intruder or not. It is used to detect only the known attacks. Unknown attacks cannot be detected using signature based detection.

Anomaly or Behavioural detection[8] is concerned with identifying events that appear to be anomalous with respect to normal system behaviour .It is used to detect unknown attacks

that are not defined in the database of the IDS.Here we use anomaly detection method to identify the intrusion that is present in the stego-image

3. RELATED WORK

WojciechMazurczyk, and Krzysztof Szczypiorski [9] The paper focuses on information hiding possibilities in cloud computing. It introduces the various steganographic communication scenarios in cloud computing which is based on location of the steganograms receiver. It also represents the threats that steganographic method can cause to the data stored in the cloud.The papers recommends for effective steganalysis methods to thwart the steganographic intrusions in cloud.

Bo Liu and Jin Wang [10] The paper deals with Audio steganography attack which is regarded as most serious attack to cloud storage systems.Audio steganography helps users to hide their secret data within regular audio files. The steganography user can transmit secret information through sending media files,which appear to be normal sound files.hackers utilize this feature to deceive the current security mechanisms (or) traditional countermeasures (egsteganalysis) for protecting cloud storage systems by hiding their malicious code in sound files and sending it to victim servers.A very little research has been done to thwart audio steganography attacks against cloud storage system.

Dai Zhonghua ,Peng Yong and Xiong Qi[11] The paper focuses on improving the accuracy of steganalysis and proposes Image steganalysis techniques based on cloud computing ,BP neural networks and supervised learning algorithm. Here the cloud computing is used as a platform to improve the efficiency of the Image steganalysis.

Bartosz Lipinski, WojciechMarurczyk, Krzysztof Szczypiorski [12] In this paper CloudSteg a steganographic method is designed which allows the creation of a covert channel based on hard disk contention between two cloud instances which is present in the same cloud instance.

4. PROPOSED FRAME WORK FOR STEGANOGRAPHIC INTRUSION DETECTION SYSTEM IN CLOUD

The proposed steganographic intrusion detection system uses traditional IDS for building StegnoIDS . It consist of the following components

- Analyser
- Detection system
- Alert system
- Responds sent to the administrator
- Knowledge base system
- Behavioural base system

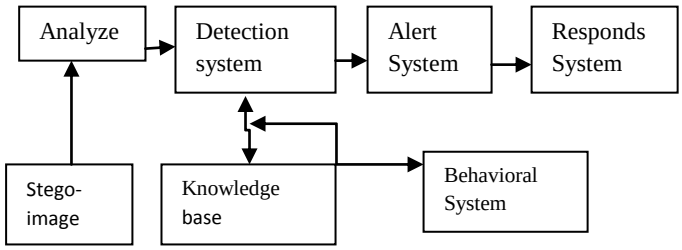

Fig 1: Components of StegnoIDS

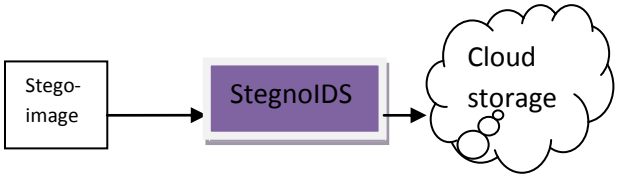

Fig 2 Proposed framework Steganographic IDS

When a user wants to store a confidential data in cloud through a stego-image .Stego-image is first examined by the StegnoIDS before it is stored in the cloud storage.

- When the stego-image enters the Analyser component of stegnoIDS the image is analysed for any changes present in the LSB of the image.If there is any changes presentin the LSB of the Stego-image it is sent to the detection system of the StegnoIDS.
- Detection component compares the stego-image with the pattern stored in the Behaviour and knowledge components.If anomaly in the stego-image is detected then a alert message from the alert component is sent to the administrator. The administrator takes necessary steps to thwart the intrusion to occur in the stego-image.
- Knowledge and Behaviour component of the IDS provides information for detecting the intrusion in the stego-image and it is frequently updated with recent patterns .

The components of StegnoIDS can be represented in a block diagram

5. CONCLUSION

In this paper we discuss an overview of steganographic threat in cloud and proposed a framework called stegnoIDS for detecting the steganographic intrusion in stego-image.Our future work is to implement the framework and to provide a efficient way of detecting steganographic intrusion which affects cloud security.

6. ACKNOWLEDGMENT

I thank my Supervisor Dr. H Srimathi, Professor,SRM University for giving guidance and support in my research .

7. REFERENCES

[1] CSA Cloud Security Alliance,"Security Guidance for criticalareas of focus in Cloud Computing"V3.0.

[2] Dawn Song,Elaine shi and Ian Fisher,Umesh Shankar, "Cloud data protection for the masses",University of California Berkely ,Google, January 2012.

[3] CSA Cloud Security Alliance,"Top threats to CloudComputing"V1.0,prepared by cloud security alliance, March 2010.

[4] D. Harnik, B. Pinkas, A. Shulman-Peleg," Side Channels in Cloud Services: Deduplication in Cloud Storage", IEEE Security and Privacy, Volume 8,Issue 6 ,November 2010.

[5] Johnson N.andJajodiaS.,"ExploringSteganography,Seeing the Unseen,"*IEEE Computer Society*, vol. 31, no.2 pp. 26–34, 1998.

[6] Chirag Modia,n, DhirenPatel a, BhaveshBorisaniya a, HirenPatel b, Avi Patel c, MuttukrishnanRajarajan""Asurvey of intrusion detection techniques in Cloud"in Journal of Network and Computer Applications 36 (2013) 42–57.

[7] Mehmood, Y. ; Habiba, U. ; Shibli, M.A. ; Masood, R. "Intrusion Detection System in Cloud computing:Challengesand Opportunities",2nd national Conference on InformationAssurance ,2013.

[8] AnimeshPatcha,Jung-Min Park "An Overview of Anomaly detection techniques : Existing solutions and Latest Technological trends",in journal of Computer Networks,51 (2007) 3448–3470.

[9] WojciechMazurczyk and Krzysztof Szczypiorske "Is cloud computing Steganography –proof"Institute of Telecommunication ,Warsaw University of Technology

[10] Bo Liu, Eric Xu, Jinwang.and more authors "Thwarting Audio Steganography attacks in cloud storage systems",published in International conference on Cloud and service computing(csc),pg259- 265, Dec2012.

[11] Dai Zhonghua,Xiong Qi and Peng Yong " Research on the Large Scale Image Steganalysis Based on CloudComputing and BP Neural Networks",EigthInternational Conference on Intelligent information Hiding and Multimedia Signal processing, July 2012.

[12] BartoszLipiński, WojciechMazurczyk, KrzysztofSzczypiorski"Improving Hard Disk Contention-basedCovert Channel in Cloud Computing Environment"Warsaw University of Technology, Institute of Telecommunications Warsaw, Poland