ISSN:2231-0711
www.ijcset.net

Enhancing Security in Cloud Access Mechanism by Establishing Covert Storage Channel

Amanjot Kaur[1], Amarpreet Singh[2]

[1]*Computer Science Department, LPU, Jalandhar, Punjab, India,*
[2]*Computer Science Department, ACET,Amritsar, Punjab, India.*
[1]er.aman_jot@yahoo.co.in
[2]amarmandeep@yahoo.com

***Abstract*- Moving computing into the "Cloud" makes computer processing much more convenient for users but also presents them with new security problems about safety and reliability. While accessing the data we follow a data policy known by third party. They can use our data. So to overcome this problem we purpose a new scheme that makes use of the covert channel technique to secure the data being communicated between cloud server and client from the third party(any process/subject).**

Keywords: **Cloud Computing, Covert Channel, CSP, Virtualization.**

I. INTRODUCTION

Cloud computing architecture consists of two parts "the front end" and "the back end". The front end of the cloud computing system compromises the client's device (or it may be computer network) and some applications are needed for accessing the cloud computing system. Back end refers to the cloud itself which may encompass various computer machines, data storage systems and servers. Group of these clouds make a whole cloud computing system. A special type of software called "middleware" is used to allow computers that are connected on the network to communicate with each other.

There are three kinds of cloud services model, namely, Software as a Service (SaaS), Platform as a Service (PaaS) and Cloud Infrastructure as a Service (laaS).[1] The basic structure of the cloud computing model as shown in Figure 1,it divided into five levels, from top t o bottom is resources provide layer, cloud services provide layer, information transport layer, professional service provider layer, end user layer. The cloud service providers (CSP) use the resources provided by resources layer and their technology (such as Virtualization Technology) to integrate the cloud services, and through the information transport layer to provide these services to users.

I. DATA ACCESS SECURITY IN CLOUD

The use of the cloud computing environment to cater to the demands of users in the internet has made data access security a critical issue in cloud computing due to the variety of IT services that can be provided through a cloud environment. While accessing the data we follow a data policy known by third party. They can use our data. So to overcome this problem we can use covert channels.

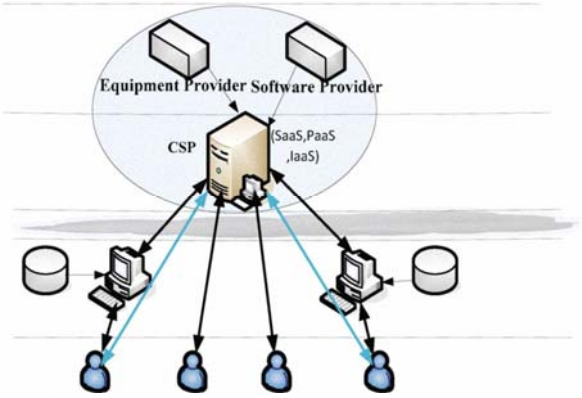

Figure 1. Users and service providers in basic cloud computing architecture.

II. COVERT CHANNEL

Covert Channels are not everywhere. However they CAN be everywhere, thus providing answers to several issues raised by the use of encryption: legal restrictions and lack of discretion. In the first case the main concern is the protection of personal privacy. One may want his communications not to become public. In the second one the issue is to have communications remain undetected. If the content of an encrypted mail should not be readable, the communication itself is not stealth. And this piece of information may be valuable, mainly if one knows that two entities tries to protect the privacy of their communication. As most security concepts, covert channels do have a dark side. As they provide a stealth and secure communication channel, they can undoubtedly be used to establish connections that are theoretically prohibited by the security policy. Then information leaks become possible as well as asynchronous command channels between the compromised system and its master. For those whose task it is to assure security, electronic communication without scrutiny that can continue between parties trying to circumvent a security policy poses a risk. This is true whether the "parties" are individuals with malicious intent or processes with different security levels passing data while running on a shared CPU. Covert communication channels have been present throughout history and continue to be developed, used and sometimes exploited by those intent on keeping their communications not only secret, but also hidden. Awareness has increased in

the application of covert channels, fueled by increased demand for development in the field of digital watermarking and fingerprinting for copyright protection and infringement prosecution, and reports of increased use for illegal purposes on the Internet. The technology itself is a double-edged sword. To understand the concept of covert channel we have to understand the meaning of two terms i.e "overt" and "covert". Dictionary meaning of Overt is open to view , not conceal, not secret and that of covert is Done Secretly,Covered, Sheltered, Hidden.Talking about channels, An *overt channel* is one which is designed for the authorised transfer of data.A *covert channel* is, by contrast, a path that can allow information to flow in a manner that *violates* the security policy of a system, allowing the transfer of information by an *unauthorised* process Covert Channels have be defined for the first time by Lampson in 1973.A path of communication that wasn't designed for [that sort of] communication between two processes. It was authorized to communicate, but not in the way they actually are.[2] According to a 1985 U.S. Department of Defense publication titled "Trusted Computer System Evaluation", a covert channel is defined as:". any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy." [3]

The fact that a communications channel is covert literally means that it is hidden. This implies that a "third party" does not know of *even the existence* of such a channel. One of the most common and perhaps the best vehicle for discussing the dynamics of covert communications is found in what is known as the "prisoners' problem" initially by G.J. Simmons in 1983.[4]

III. TYPES OF COVERT CHANNEL(OVERT CHANNELS)

Covert storage channel-Involves the direct or indirect writing to storage location by one process and direct or indirect reading of the storage by another process. They typically involve a finite resource (e.g. sectors on a disk) that is shared by two subjects at different security levels. They use an attribute of a shared resource to send/lead information. Covert Timing Channels-Signals information to another by modulating its own use of system resource is such way that this manipulation affects the real response time observed by second process. They use a temporal or ordering relationship among accesses to a shared resources to send/lead information.*[3]*

Legitimate Uses of Covert Channels?

Information and communication dissimulation is not a new topic. However applications remains numerous and most recent techniques make such channels more difficult to detect. This can be a good thing if covert channels are used to protect privacy or increase security of critical communication. However when applied to security policy bypassing, information leak or compromised system control the knowledge of such technique becomes mandatory to enhance detection engine. It is worth noting that, as with any technology, CCs may arguably be used for good. A person or group whose web traffic is being monitored by an oppressive state might use CCs to access blocked content. This would naturally require outside cooperation in the form of a 'translation server' to which the tunnel would be directed.CCs, as we have seen, could offer communication completely hidden from the view of the watchers. In our paper we are proposing this legitimate use of covert channels.

IV. THE PROPOSED CONCEPT

In cloud environment there is a great security concern when it comes to data communication between clou server and client. There are chances that any third party can intervene this communication between the two parties (cloud server and client) and can steal their data.

We propose a scheme which establishes the covert storage channel communication between cloud server and client in a legitimate manner so that third party is unaware about this. As we know that :Covert storage channel-Involves the direct or indirect writing to storage location by one process and direct or indirect reading of the storage by another process.

- Typically involve a finite resource (e.g. sectors on a disk) that is shared by two subjects at different security levels."
- Uses an attribute of a shared resource to send/lead information.

The idea is to embed information in certain header fields of Ipv4 header that are either unused, immutable or mutable with certain predictability. The embedded information is carried out of the network with the intention of avoiding detection by the third party. Information may be placed in the payload section of the packets. A number of header fields have been proposed for concealing the information. Several IPv4 header fields will now be considered:

- Type of Service: This field holds 8 bits of information that can indicate quality of service parameters to routers on a packet's path.
- IP Identification: This is used in the reassembling of datagram when fragmentation has been used. This field contains 16 bits and could yield a high capacity for transferring information. The only constraints on the value of this field are uniqueness over the length of time that fragments of a packet might reasonably remain in a network. Several schemes have been devised that make use of a pseudorandom sequence to embed data.
- IP Fragment Offset: When IP packets are fragmented, each fragment contains an offset field to allow for the reassembly of the packet. Information can be transmitted by modulating the size of the fragments originated by the host, and thus the offsets.
- IP Flags: This flags are either Do Not Fragment (DF) or More Fragments (MF) which is 0 if the fragment is the last, or if no fragmentation has taken place. It is possible to be able to use these flags but if the context of the packets is analysed it may be obvious that the value should be zero. This channel

is obviously very limited in the capacity that it can generate.

- The Type of Service field within the IP header.
  - Bits used for differentiated services.
  - These bits can prioritise traffic according to nature of traffic being carried.

If the site is not using DiffServ then the bits should be set to zero and this would clear the channel and maintain the integrity of the header.

If DiffServ is being used then zeroing will destroy Diffserv and break protocol. Thus there is a potential problem of normalising this field but if DiffServ is being used normaliser may be able to detect this if for example it is Network-Aware.

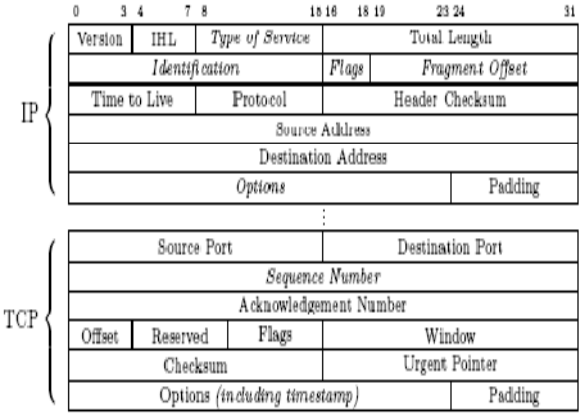

Fig 2: TCP/IP Format

REFERENCES

[1] Tian-li-qin, Lin chaung, "Evaluation of User Behavior Trust in Cloud Computing" 2010 International Conference on Computer Application and System Modeling (ICCASM 2010).

[2]Lampson, B.W., A Note on the Confinement Problem. Communications of the ACM, Oct.1973.16(10):p. 613-615.

[3] U.S. Department of Defense. Trusted Computer System Evaluation "The Orange Book". Publication DoD 5200.28-STD. Washington: GPO 1985

[4] Simmons, Gustavus J. Prisoners' Problem and the Subliminal Channel (The), CRYPTO83 - Advances in Cryptology, August 22-24. 1984. pp. 51-67.