Secure video steganalysis to detect hidden communication between virtual machines in cloud

Shwetha B N
PG Student
Dept of CSE,Cit, Gubbi,Tumkur.

Prof. Shantala C.P
Vice Principal and HOD,
Dept of CSE,Cit,Gubbi,Tumkur.

Girish L
Assistant Professor
Dept of CSE,Cit Gubbi,Tumkur

***Abstract* —Cloud computing provides various advantages for its users. Because of its security problem cloud is lagging behind. At present communication between physical machines can be done easily but problems in communication between virtual machine is less developed. . In our work, we are proposing a efficient method for the virtual machine communication detection by using steganography and steganalysis. Through the covert channel safe communication can be achieved between the virtual machine. If attacker extracts the organisations secret data and send to the other person who is present outside the organisation by embedding the secret information in video and by uploading that into the cloud service like you tube, then the SDN controller checks the packet against flow table entries if there is a match then it will drop the packets and send notification to admin if there is no match video can be downloaded by other users normally.**

This paper uses the Software defined networking which is a new technology that proposes the isolation between the control and data plane from the given network.Control plane will decide how packets should be forwarded and data plane will actually forward them. SDN requires some method or interface for control plane to communication with data plane. One such mechanism is called as OpenFlow.

***Keywords* —Video steganography, Hidden communication, Steganalysis, virtual machine,Data exfiltration.**

I. INTRODUCTION

In a present days cloud computing is very popular and it is still evolving standard. It is strong growing area in a computing research and industry today. Cloud computing is on demand service where information, shared resources, software and other devices are given according to client requirements specific time. Cloud is a term which is used generally in case of internet. In this environment users need not to own the infrastructure for different computing serviceshere users can access their data from any computers and from any part of world.

Several services and models make cloud computing advantageous and accessible to the end user. It has two models they are: Deployment model and service model. Here deployment model has three categories i.e., public, private, and hybrid cloud. private cloud is also known as internal cloud or corporate cloud which makes the Corporate network. Private cloud is used in an organization that needs more control over their data compared to that is provided by the third party organization. Public cloud gives services to anyone with the help of the internet. Here in public cloud business rents capability and they will pay for what they use. Hybrid cloud is the merger of private and public cloud.

Service model provides three types of services i.e., Infrastructure-as-a-service[Iaas],Platform-as-a-service[Paas] and Software-as-a-service[Saas]. Here in Iaas only network is provided where as in Paas network and operating system is provided and in Saas operating system, required software and network is provided. Cloud service is popular because it reduces the convolution of network, users do not need to buy software licenses and information in cloud is not easily missing.

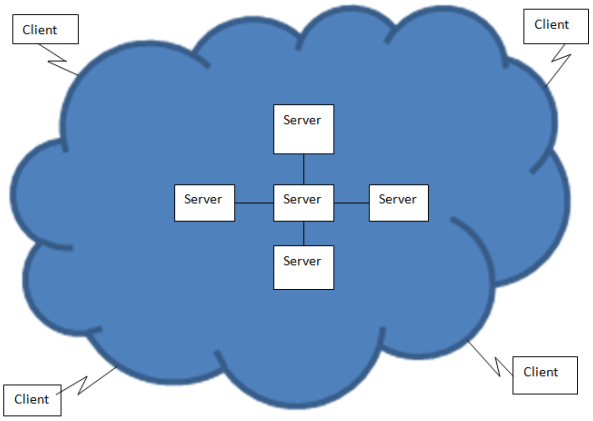

Fig. 1: Cloud architecture

Above fig shows the architecture of cloud here particular users join to cloud from their own personal computer over the internet. For these particular users, the cloud will be visible as a single application. Hardware in the cloud and also operating system that maintains the hardware connection is not visible.

To perform the hidden communication between virtual machines steganography is used. Steganography is the method of communicating in the form which conceals the presence of communication. In opposite to cryptography, where the enemy is permitted to identify, alter the messages without the knowledge of cryptographic sender and receiver. But in the steganography the goal is to conceal the message within other harmless message. In this way it does not permit the enemy to even identify that there is another message. There are different methods in steganography Text steganography, Image steganography, Audio steganography, video steganography. Depending on the format of file on which message are encoded.

ISSN: 2278 – 1323

Steganographic techniques be used to provide perfect tool for hidden communication among the secret parties. The main aim of all these technique is to conceal the secret data in a innocent looking carrier it means as in the normal transmission of message of the users. Based on the extent of the covert channel which can be created it may be network or local covert channel. In the network covert channel communication is done secretlythrough the network. In the local covert channel the extent will be limited to the single physical machine.

Covert channel is the medium for steganographic communication. Covert channel means hidden channel. This suggests that "third party" cannot know even the presence of such channel these acts as a path to communicate the message. Good carrier for hidden data exchange should have two features: it must be popular it means use of such carrier must not introduce a abnormalities. Other feature is alteration of the carrier after inserting the steganogrammust not be visible to the other party who is incognizant of the steganographic method.

Data Exfiltration [1] is the unauthorized copying , extraction or displacement of data from the computer. Data exfiltration is the mischievous activity done through different techniques. Typically with the help of internet due to this data exfiltration attacker can extract the sensitive information from the organization

Now a day's maintain of the network systems are becoming more critical, and also controlling the network manually is becoming more challenging because of large amount of growth in network infrastructure, Because there is a need of go to that network node, and to solve that trouble by the method of vender specific solutions ,and after that debug that error, so to overcome this network difficulties new technology called software defined networking is used.

SDN[13] decouples the Network plane into control plane and data plane. Control plane can be programmable.SDN needs a method or interface for communication between control plane and data plane. open flow protocol is one such mechanism. control plane take decision about how packets has to be forwarded but data plane forwards the packets.

Whenever packets containing secret information arrives at the SDN controller it will automatically detect the presence of the secret information and drop the packets by informing to admin.

II. RELATED WORK

Hidden communication in cloud computing environment is present day research field which has already drawn the recognition of research community. The first paper that proposed the hidden communication in cloud computing was in2009 by Ristenpart et al.[2].Large number of papers are depend on the foundation that his work provides. Cross virtual machine data leakage is due to the commonly shared resources this is the way in which local covert channel is created which enables one way or two way data exchange.

There are different methods of steganographic techniques. Each of this is having its own advantages and disadvantages. Text steganography [3] has different approaches where in the Line shift method, if text is retyped the secret information will get destroyed. In the word shift method also if the text is retyped the secret information will be lost. In the Syntactic method users can notify the abnormal use of punctuations. In the missing letter puzzle method file will have large number of question marks this will attract third party easily. In the edge Adaptive Image steganography method smooth or flat regions is also contaminated by the insertion of hidden data. In the image steganography LSB method [4] both 8 bit and 24 bit images are having their own disadvantages. In the 8 bit image only 256 possible colours are there. In 24 bit image format the drawback is, it is very large in size hence it has to be compressed. In the Audio steganography [5], in LSB method data loss will be there due to channel noise.

III. PROPOSED SYSTEM

Inthe proposed system hidden communication between virtual machine is detected by using video steganalysis

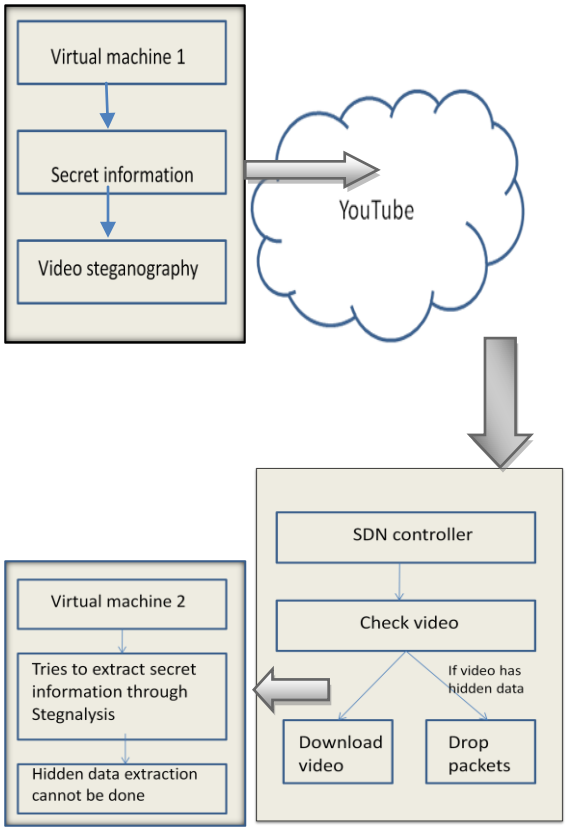

Fig. 2: Architecture of proposed system

In the proposing system virtual machine 1 will perform the steganography technique where virtual machine 1 will extract the secret information from the organization and with the help of video steganography technique it will hide the secret information. For this purpose video will be divided into packets and in the unused place of payload the secret information will be added. And the entire video will be uploaded to the youtube[12].

ISSN: 2278 – 1323

SDN controller present in the youtube will perform the checking options. Where SDN controller will check the incoming packets against flow table entries if match is found that is packet contains thenother than video codec information then it will drop the packets and send notification to admin and also it will play the secret information.

If the video does notcontains the hidden information then it will transferred to the destination that is virtual machine 2.It will perform the steganalysis technique to extract hidden information but the hidden information will not be played.

Through the advent of software defined networking [6], The network itself can be used as the observation point of forensic system and system administrator is able to ascertain the correctness of every system when issuing a forensic query, making it possible to detect the presence of previously unobservable attacks.

It is very hard to view the behaviour of network host system by the administrator in the current traditional network system so SDN disconnect the network plane as dataplane and control plane, control plane can be forensic analysis.

Within the constriction of corporate network, network provenance can be used to outline the traffic and find out the cause of incident. Example admin can employ a network provenance system to find out if apprehensive routing table entry is because of simple configuration.

Network provenance system is used in distributed system to discover faults and attacks. These methods depend on the correct nodes to monitor and record the procedures of other nodes. Drawback of this method if attacker watchfully avoids the interaction with the nodes, the attacker may not become invisible to forensic system.

This is trouble for stored sensitive information in a private network if the information is exfiltrated to cloud sharing video service link you tube. The provenance system maynot detect the node which leaked the information until the leakage is detected by proper node.

Instead of depending on the reports given by the end nodes, all network links can be converted into as a reporting tool with the help of the programming a distributed group of SDN switches with middle boxes [7] .but achieving such a act in traditional network system is costly and also complex, needing a proxy boxes between all nodes in network. Depending on the group og flow tables rules which are programmable. SDN permits to carry out complicate set of operations on the packets when it enters the switch. By performing pattern matching in packet headers dropping of the unauthorized communication can be done.

With the help of software defined networking in the data exfiltration, admin of the private network can be beam the entire network in laptop and control the network with the help of programming.

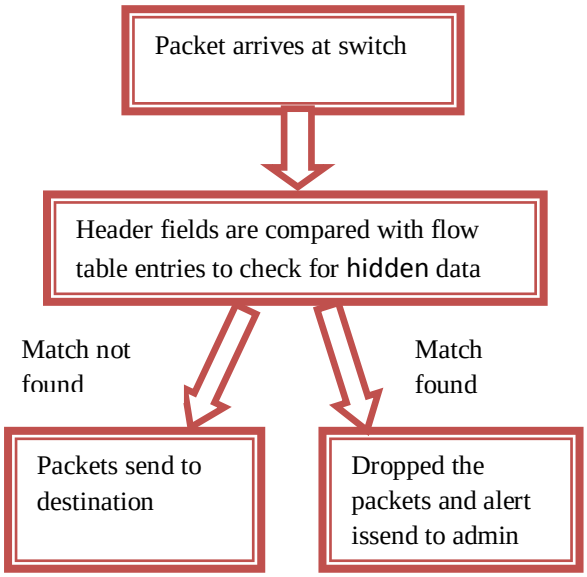

Fig. 3: SDN based forensic system

As shown in the figure 3 whenever the packets arrives at the switch its header fields are compared to flow table entries to check whether there is a hidden data if match is found then packets are dropped and alert message will send to the admin. If there is no match then packets will sends to the destination.

When the stream of video is transcoded the actual payload size is purposely unaltered and changes in the codec is not signified. After allocating the transcoded video payload the left free space is filled with secret data. Hence it is very hard to identify the hidden communication for this method with the help real time transport protocol [RTP] [8] header admin can detect the data exfiltration of video steganography.

IV. IMPLEMENTATION

The implementation process consists of three modules.

- Video steganography
- SDN controller
- Steganalysis

A. Video steganography

Video is the technique of electrically recording, transmitting, saving , catching and reconstructing the array of still images that acts as scene which is in the movement. In the videos rate of frames [9] , number of still images per unit time is measured. Video quality can be identified by various techniques or using expert observation.

Attackers now a days choosing the video steganography for data exfiltration. In the video steganography module the secret message must be hidden inside the video. The large size of video is more advantageous in this case because it allows large amount of data to be hidden inside the video. It consists of three parts.

- Cover video
- Secret message
- Stego video

ISSN: 2278 – 1323

Cover video: The video which is used as carrier for the embed message into.

Secret message: The sensitive information which has to be transmitted to the destination by hiding it in the video.

Stegovideo: It is the video which has hidden message within it. So given a cover video and a secret message. The attacker produce the stego video by the cover video by using steganographic technique.

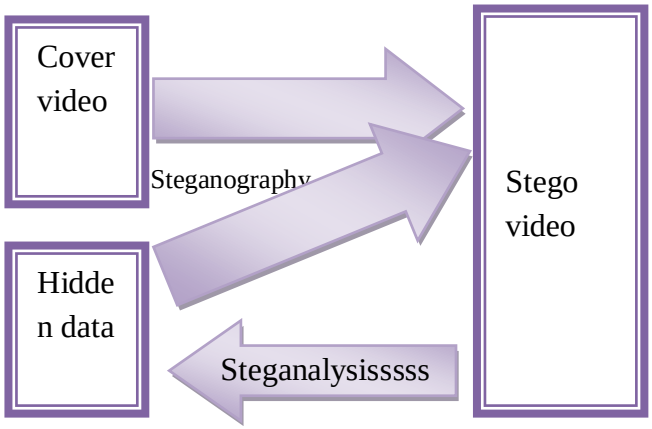

Fig.4:Video steganography model

The stream of the video has a cluster of frames and secret message which has to be hidden in the frames in the unused parts of the payload the cover video will be broken in to frames then unused parts of the payload is determined and the secret data will be added into that. The message size will not considered in the video steganography because secret message can be hidden in multiple frames and then it is uploaded into the cloud sharing service like youtube.

B. SDN controller

Whenever the video packets arrive at the youtube the SDN controller present there will perform the checking actions for the hidden data. Opendaylight is the SDN controller used here. The main character of the SDN is, it decouples the control plane and data plane so in order to make communication between them openflow protocol is used.

1.Openflow: Openflow[10] is regarded as the first software defined networking standard. It acts as a communication protocol in the SDN that makes SDN controller to communicate with the forwarding plane and it can make necessary modifications to the network thus it can adjust with the altering business requirements.

If anyone wants to work in openflow environment if any machine has to interact to an SDN controller it must support the openflow protocol with the help of this interface the SDN controller make changes to the flow table permitting network administrator to control flows and traffic.

Openflowcreates flow table [11] entries in switches hence switches can take the necessary actions. Based on the actions the openflow architecture describes three main concepts:

- The network which is created by openflow compliant switches [14] that create data plane.
- The control plane which has openflow controllers.
- Secure control channel that joins the switches to the control plane.

Openflow compliant switch is a fundamental device which pushes packets depending on the flow table. Flow table has a set of entries which may be packet header, action and statistics.

Packet header : Defines the flows.

Action : It describes the manner in which packets has to be processed.

Statistics: It has number of packets count and the time when final packet matched with the flow.

2.Opendaylight: Opendaylight is the SDN controller which is using. An SDN controller acts has the brain of the SDN network. Sending information to the router and switches below through the southbound API and the application and business logic present above it through northbound API .

The main responsibilities of opendaylight are:

- It gives way to control and cooperate with underlying platform such as openflow switch.
- It must know the way to interpret the information send by the openflow switch.
- It must offer the all instruction depending on the specifications which may be optional and required to perform programming of the switch.
- Should specify the method to poll the switch for different details and must be interpret the response.

C. Video steganalysis

It is last module where once SDN controller detects the match, which is found by the packet with the flow table entry, it performs the steganalysis. Where during this method it extracts the hidden information from the video and plays the hidden information and drops the hidden informationspackets by sending notifications to admin before that is reaching the hands of other attacker.

V.RESULT ANALYSIS

Results are analyzed for audio files of different sizes and the numbers of frames are calculated and the time for that also calculated. The audio files are added into the payload field in the packet .payload field in the packet has the actual video codec. In the unused parts of payload the audio file is added.

In the Result analysis depending on the size of the audio file selected video will be divided into frames. If the size of the audio file is large then it will divide into large number of files and it takes more time to divide.Results are tabulated as in the table.

ISSN: 2278 – 1323

Tabel 1: Analysis of Results

Secret Audio fileSize	Number of frames	Time
591Kb	110	00:01:50.00
1.5Mb	283	00:04:43.00
1.9Mb	351	00:05:51.00
4.3 Mb	797	00:13:17.00
4.9Mb	902	00:15:02.00
6.9Mb	1280	00:21:20.00

When graph is plotted by taking number of frames in x axis, time and bitrate in y axis the results will be as shown below:

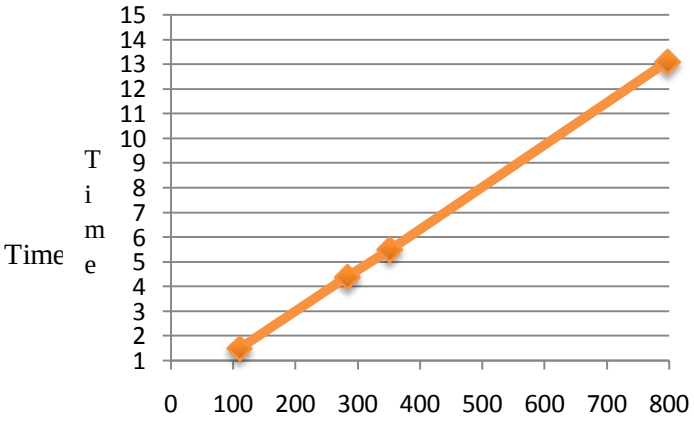

Fig.5: Graph showing the variation of time based on number of frames

VI. CONCLUSION AND FUTURE WORK

In this paper, we have investigated the problem with video steganography,which is very dangerous in private corporate network. To ensure the security of the sensitive data in compromised network we proposed an effective steganalysis strategy by using the software defined networking. Where video with sensitive information is dropped automatically.By giving notification to admin about the video with hidden data. With the help of SDN framework administrator can control the network by programming. In this method if the data is exfiltrated by one virtual machine and uploaded to a remote adversary like cloud video sharing service such as YouTube,it can be detected and dropped before reaching the other virtual machine. Through the detailed analysis, we have seen that our scheme almost guarantees the security of the sensitive data.It is possible to detect video steganography only in some formats of videos. So it can be enhanced in the future to detect in all video formats.

ACKNOWLEDGMENT

We are grateful to express sincere thanks to our faculties who gave support and special thanks to our department for providing facilities that were offered to us for carrying out this paper.

REFERENCES

[1] Iftach Ian Amit, “Advanced Data Exfiltration–the wayQ would have done it”, iamit, September 2011.

[2] T. Ristenpart, E. Tromer, H. Shacham, S. Savage, “Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds”, Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS‟09), November 2009

[3]MonikaAgarwal,”TEXT STGANOGRAPHIC APPROACHES: A COMPARISON”, International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.1, January 2013.

[4] Sadoon Hussein Abdullah, “Steganography Methods and some application (The hidden Secret data in Image)”, April 2009.

[5] Jayaram P, Ranganatha H R, Anupama H S,” INFORMATION HIDING USING AUDIO STEGANOGRAPHY – A SURVEY”, The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011.

[6] ShridarKNRao,“SDNandItsUseCase-NVandNFV” NTIL2014.

[7] https://www.sdxcentral.com/resources/sdn/sdn-controllers/sdn-controllers-comprehensive-list/

[8] WojciechMazurczyk, PawełSzaga, Krzysztof Szczypiorski, “Using Transcoding for Hidden Communication in IP Telephony”,Multimedia Tools and ApplicationsJune 2014, Volume 70, Issue 3, pp 2139-2165.

[9] K.ParvathiDivya, K.Mahesh,” Various Techniques in Video Steganography -A Review”,International Journal of Computer & Organization Trends – Volume 5 – February 2014.

[10]https://www.sdxcentral.com/resources/sdn/sdn/whatis-openflow?/

[11] Wolfgang Braun * and Michael Menth,” Software-Defined Networking Using OpenFlow: Protocols, Applications and Architectural Design Choices”, May 2014.

[12]https://www.youtube.com/

[13] Sandra Scott-Hayward, Gemma O’Callaghan and SakirSezer, “SDN Security: A Survey”.

[14] Nick McKeown, Tom Anderson, “OpenFlow: Enabling Innovation in Campus Networks”, March 14, 2008

ISSN: 2278 – 1323

First Author: Shwetha B N was born in Karnataka, India. She received the B.E Degree in Computer Science and Engineering from Visvesvaraya Technological University Belgaum Dist., India in 2013 and pursuing M.Tech Degree in also same branch and University. Her research interests are in the area of cloud computing, SDN and steganography

Second Author : Prof. Shantala C.P. received the BE and M.Tech degrees both in computer science and engineering. She is working as Vice principal andHead of the Department at Chanabasaveshwara Institute of Technology, VTU University. Her Research interests including Steganography, Network Security,Cloud Computing and Brain computer interface.

Third Author: Girish L was born in Karnataka, India. He is working as Asst.Prof. in Computer science and Engineering Dept., CIT, Gubbi, Tumkur (district), Karnataka, INDIA. His area of interest are steganography ,cloud computing, SDN, Big data

ISSN: 2278 – 1323