Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 6, June 2013, pg.256 – 261

RESEARCH ARTICLE

Data Protection for Clients in Private Network through Virus-Protection as a Service

Manivannan Palanivel[1], Murali Prasath[2]

[1]Department of Computer Science Engineering, Sona College of Technology, Anna University, TamilNadu, India

[2]Department of Computer Science Engineering, Sona College of Technology, Anna University, TamilNadu, India

[1] pvmrules@hotmail.com; [2] muralivprasath@gmail.com

Abstract— Cloud computing is seen as the next wave of Technology which will accelerate the pace of the IT industry. Cloud services will increase the computing power without investing much on infrastructure. The cloud offers service includes SPI – Software, Platform and Infrastructure. Cloud services enable users to remotely utilize the services in the pay-per use model. As the services types evolve, the need of the security shoots up. The aim of this paper discusses how to provide Security as a Service (SECaaS). Conventional virus protection applications are standalone and needs individual updates .The idea of providing Virus Protection as a Service(VPaaS) is discussed as a part of SecaaS .This centralized virus protection in cloud will serve as a one point Anti-virus application which will secure the clients in the network against virus attacks. This model can be seen as a successful business model for the organization and also reduce the cost of individual license for the applications.

Key Terms: - Cloud computing; Software as a Service; Virus Protection as a Service; Openstack; Virtual machine

I. INTRODUCTION

Cloud computing is the manipulation of hidden computing resources that are provided as services to the clients through the internet. A cloud can be public, private and hybrid. A public cloud can be accessed by anyone who is using the internet. A private cloud is a closed network that supplies deployed services to a limited number of people. Virtual private cloud is offered as a commercial computer service through public cloud. the goal of cloud computing is to provide easy, flexible and reliable access to computing resources and software services. A hybrid cloud is a combination of private and public cloud. This works by leasing a extend services to the private cloud. The availability and flexibility of free open source cloud platforms are mainly used to deploy the private and hybrid cloud computing environments. Software as a service is a type of service model in which the software and its libraries are centrally hosted and the clients can access the resource. as a part of SaaS providing SECaaS can be successful business model. Security includes features like access management, data loss protection, web security, email security etc.

A. Characteristics[11] and Benefits Of Cloud

Cloud computing has a variety of characteristics and advantages, with the main ones being:

1) *Utilized Infrastructure:* The utilized infrastructure enables the sharing of physical services, storage, and networking capabilities. The cloud infrastructure, regardless of deployment model, seeks to make the

most of the available usage of its infrastructure across a number of users and it means there will be no wastage on utilizing the hardware potential.

2) *Based on Requirements:* The clients can use the cloud service if there is any current demand requirement. So they don't need to pay all the time. This is done automatically using software automation, enabling the expansion and contraction of service capability, as needed. This dynamic scaling needs to be done while maintaining high levels of reliability and security.

3) *Network Access:* It can allow access across the internet from a broad range of devices such as PCs, laptops, and mobile devices. Deployments of services in the cloud include everything from using business applications to the latest application on the newest Smartphones.

4) *Billing:* Cloud service providers uses metering for managing and optimizing the service and to provide reporting and billing information. In this way, consumers are billed for services according to how much they have actually used during the billing period.

Mobile Accessible: Use of mobile phones in today's world is mandatory. It is going to be the computer of the present and near future. So there is a need for the cloud service provider to build a service that can be supportable in mobile phones.

II. SECURITY AS A SERVICE

Security as a Service in cloud allows securing the host system remotely. It is a type of computing which is used to secure all other types of computing. There are many categories [14] available in Security as a Service. They are Identity and Access management, Data loss prevention, Web security, E-mail security, Security assessments, Intrusion management, Security Information and Event management, Encryption, Business continuity and Disaster recovery and Network security. As the service from the centrally hosted server, It is easy to keep track of every new threat and so that it maximize clients system protection. There are many benefits from the Security as a Service. They are flexibility, faster scanning of user data, web interface to manage our system auditing and on-going activities from anywhere, greater security expertise and outsourcing of some administrative tasks to save time. These kinds of service are easy to deploy and requires less provisioning because it is a real time protection.

III. EXISTING SYSTEM

In the standalone anti-virus system, users have to download the anti-virus application as a contract for a specific period. The users have to get the virus definition update for a specific time interval. These update will provide the information about the virus, malware etc. This will definitely utilize a lot of disk space and ram. Because of these issues, cloud anti-virus was born. In this system, clients have to upload all their files to cloud server and the cloud server will scan the files. This system reduces the disk space usage but it requires high internet service to utilize this service. In these proposed system, clients don't have to upload the files, cloud server can scan the client disk because it is provided as a service. It will increase our protection for sure.

A. Panda:

Panda[11] is a cloud based anti-virus which is light, secure. It is capable of detecting virus, Trojans etc. It is providing ultimate security by real-time protection and collective intelligence. The present generation offers behaviour analysis and behavioural blocking. Expectations shows that next generation cloud antivirus may provide automated data processing where the anti-virus can be used in offline mode by virus definition update.

B. McAfee:

McAfee[9] secures the email services against virus, spam, zero day protection and many other threats through email encryption, email archiving and email security via cloud. Mcafee only provides the protection towards web and email services but not as real time protection for system. Mcafee includes cloud-based malware defection, disinfection and it will secure the host system even without internet by getting virus-definition update.

C. AVG:

AVG[12] is a cloud based admin platform to provide security by filtering out the virus, malware, etc. It is capable of filtering the virus by scheduling. It can be accessed from any type of browser without any proxy. It has the ability to secure the email and web transaction, but not any system through cloud.

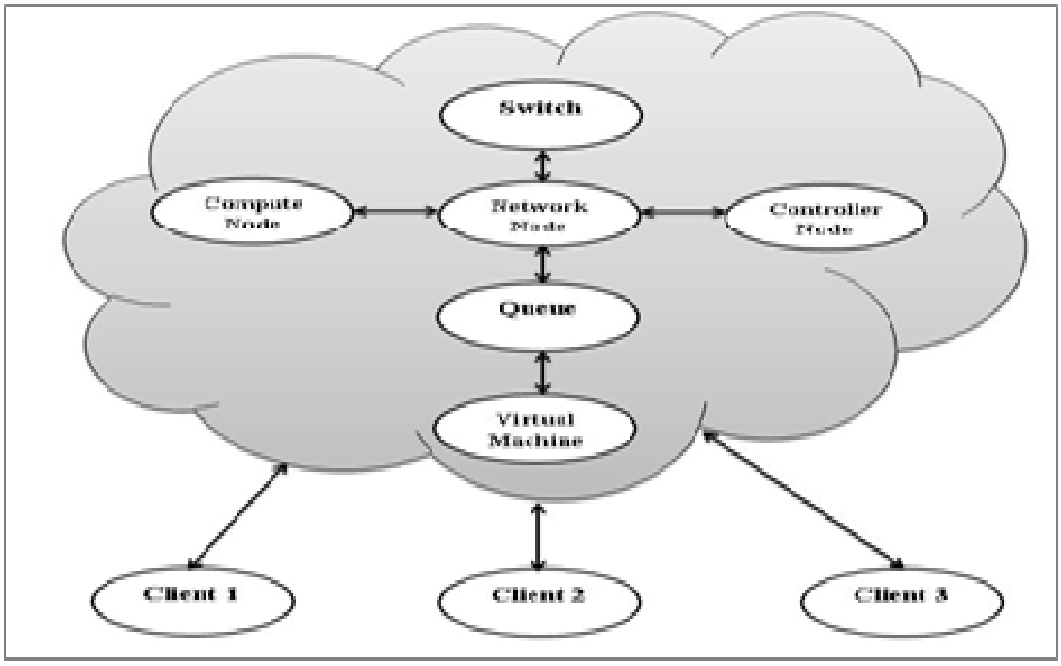
D. Symantec:

Symantec[10] gives sufficient protection to the host system and eliminated the need to manage hardware and software. It will protect the web and email exchange and also has the ability to secure the critical data by automatic streaming to Symantec server.

IV. VIRUS PROTECTION AS A SERVICE

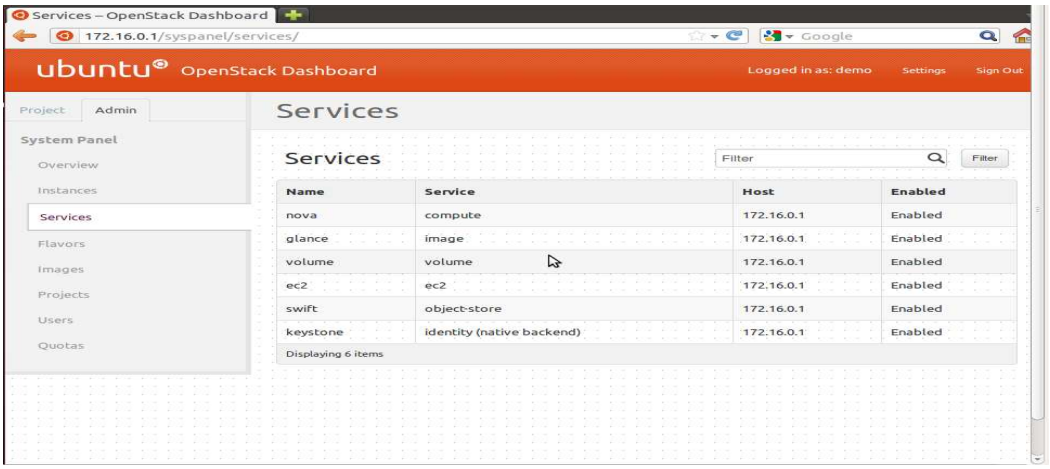
Cloud antivirus[1] is a type of anti-virus that uses lightweight software on the host computer, while it will process all the majority of data analysis to the cloud server. As antivirus is installed in the standalone system, it is hard to keep track of every known virus in the world. Because of this disadvantage, the anti-virus has been transferred as a cloud service because of this every malicious code, virus and bots can be tracked and then it is very easy to identify and remove virus from the client system. One approach to implementing cloud antivirus involves scanning client files using multiple antivirus engines on the cloud server. This paper advocates a new model for malware detection on end hosts based on providing antivirus as an in-cloud network service. Because of the proposed system, it will improve the scanning speed because of parallel computing in the cloud and it will save a lot of space in the user system and also a lot of money for the individual and for the organization.

V. INFRASTRUCTURE DIAGRAM



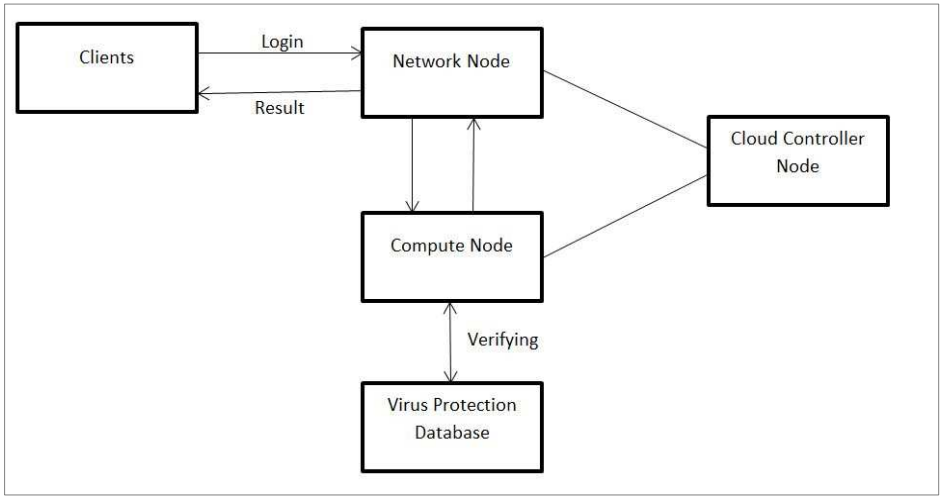
VI. OPENSTACK

OpenStack[13] is free open source Cloud computing platform originally released by Rackspace and NASA, which is mainly used to create and innovate the cloud platform for both individuals and organization. It is used to create the nodes for the cloud environment. Compute node stores and retrieves disk files and associated data in Image. Network node provides virtual networking for the available nodes. Block Storage node provides storage volumes for Compute. Image node is mainly used to store the actual virtual disk files in the Object Store. All the authentication related services will happen with Identity node. The Compute node is built on a messaging-based architecture, which allows running the services on multiple servers. Compute node transfer the message using the Advanced message Queue Protocol (AMQP) and it will use asynchronous calls to avoid blocking. Quantum is an OpenStack[7] project to provide "Connectivity as a service" between connected devices managed by other nodes in the openstack. Swift is a storage system used to provide lots of storage. Nova is used to manage and schedule the available compute resources. The OpenStack Dashboard provides administrators and users a graphical interface to manipulate the cloud server and its administrative tasks.



VII. IMPLEMENTATION

Due to many disadvantages in the standalone systems[1], many organization are planning to deploy the cloud-based antivirus. Cloud-based antivirus can be invoked by using Openstack. For building a cloud server, there are three nodes which are mandatory. Those nodes are compute, network and cloud controller node. In the compute node, the client data will be manipulated. The network node will help to control the data transmission. Cloud controller node will control the cloud server. All the packages for these nodes will be installed through internet. There will be a switch to transfer the data between compute and network node. The clamAV antivirus package will be installed on the virtual machine formed by openstack. As this open source anti-virus will be so helpful in detecting and clear all types of virus. There are many types of virus available in the computing world. They are boot sector virus, browser hijacker, direct action virus, file infector virus, macro virus, multi parties virus, polymorphic virus, resident virus, web scripting virus and many more. These viruses can be cleared at any time on the client system if the update is maintained periodically. Once the system is deployed means, the data transaction will be controlled by network node, the whole cloud structure will be controlled by cloud controller node and the client data is processed at compute node. As many as number of clients can be added to the cloud server depending on the compute node. There are many types of platforms available in operating system. On those the main platforms are windows, Mac, Linux. Virus Protection as a Service can be utilized by any platform by using the internet. The client can access the service by three modes[10] of operation. They are transparent mode, warning mode and blocking mode. In the transparent mode, the service is completely transparent to the client. In the warning mode, access to a file is blocked until the scan is completed. In the blocking mode, access to a file is blocked during scanning and if the file is classified as suspicious then access to the file is denied and the user is informed with an error dialog.

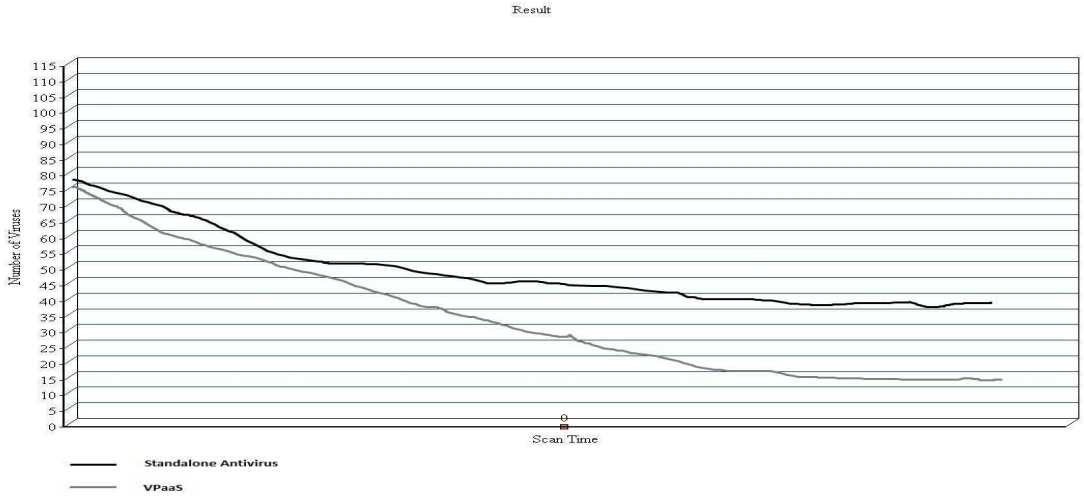


VIII. RESULT

Once the server is deployed, the clients can make use of Virus Protection as a Service. The service can be utilized as pay-per use model, just like paying for the drink and not for the cup. The server can keep the virus definition up-to-date by connecting to centrally globalized virus database, So the clients don't need to care about any virus or threats that become as vulnerability to them because of updation in the server. The cloud server will store all the infected files in one of the nodes directory, So that the clients can store the mandatory files for a specific period which they feel as needed. This will ease out the operation of clients like updation, installation and maintenance. The scan result will produce the number of scanned files and directories, infected files, known virus, version number and time in the clients terminal. Thus a option to protect the data in the private network for client has been provided by using VPaaS.

```
/root/.goutputstream-E4HITW: Empty file
/root/.goutputstream-2Q1TTW: Empty file
/root/.viminfo: OK

----------- SCAN SUMMARY -----------
Known viruses: 2186122
Engine version: 0.97.7
Scanned directories: 1
Scanned files: 21
Infected files: 0
Data scanned: 126.58 MB
Data read: 31.72 MB (ratio 3.99:1)
Time: 15.944 sec (0 m 15 s)
```



IX. FUTURE WORKS

As many numbers as clients can be added to cloud server by using virtualization. Virtualization is a concept of virtual form of anything such as software, platform and infrastructure. Now Virus Protection as a Service has been invoked and in future it can be extended to exploit as a Service, Encryption, Data Protection.

X. CONCLUSION

To address ever-growing concern of security in the IT organisation, a new business model has been proposed to implement the anti-virus using cloud. Because of this business model, it will open up a new platform for the security in IT organisation. In the standalone application, the user has to buy separate license for every system and it is very expensive for large organisation. Because of the effects in the standalone system, the organisation will deploy the proposed cloud anti-virus which is very cost effective.

REFERENCES

[1] Jon Oberheide, Evan Cooke, Farnam Jahanian "CloudAV: N-Version Antivirus in the Network Cloud ," University of Michigan ,2008

[2] Jon Oberheide, Evan Cooke, and Farnam Jahanian. Rethinking antivirus: Executable analysis in the network cloud. In 2nd USENIX Workshop on Hot Topics in Security (HotSec 2007), August 2007.

[3] Gartner,Inc.Forecast:Securitysoftwareworldwide,2006to2011,update,http://www.gartner.com/DisplayDocumentref=g_search&id=510567&subref =advsearch, 2007.
[4] Vinod Yegneswaran, Paul Barford, and Somesh Jha. Global intrusion detection in the DOMINO overlay system. In Proceedings of Network and Distributed System Security Symposium (NDSS '04), San Diego, CA, February 2004.
[5] F-Secure Corporation. F-secure mobile anti-virus. mobile.f-secure.com/, 2007.
[6] Jian Guo, Zhao-Meng Zhu, Xiu-Min Zhou, Gong-Xuan Zhang "An instances placement algorithm based on disk I/O load for big data in private cloud" International Conference on Wavelet Active Media Technology and Information Processing, 2012.
[7] Wuhib, Fetahi "Dynamic resource allocation with management objectives and Implementation for an OpenStack cloud" 8th International Conference on Network and Service Management, 2012.
[8] Shaikh, Rizwana, Sasikumar "Trust framework for calculating security strength of a cloud service" International Conference on Communication, Information & Computing Technology, 2012.
[9] McAfee Security as a service "http://www.mcafee.com/us/products/security-as-a-service/index.aspx", 2013
[10] Symantec.cloud"www.symanteccloud.com/en/in/globalthreats/learning_center", 2012
[11] Panda cloud protection "http://cloudprotection.pandasecurity.com/",2013.
[12] AVG Cloudcare "http://www.avg.com/us-en/cloudcare",2013
[13] Introduction to open stack cloud computing, Dialogic Corporation, 2010.
[14] Cloud security alliance https://cloudsecurityalliance.org / research/secaas/", 2012.

