****

**REPORT OF PROJECT**

**IMPLEMENTATION OF A CLOUD-BASED ANTIVIRUS AND STUDY OF ITS BENEFITS IN COMPARISON WITH TRADITIONAL ANTIVIRUS**

**Selected Topics in Distributed Computing (SKR 5800)**

Ali Falsafi(GS27192),Ghazaleh Rezayat(GS29087),Mohamad ali Iravani(GS27319),Shirin Nazemoroaya(GS29086) ,Vahid Moraveji Hashemi(GS28610)

**DR.AZIZOL B HJ ABDULLAH**

**Implementation of a cloud-based antivirus and study of its benefits in comparison with traditional antivirus**

***Abstract*: due, to the significant increase of cloud usage necessity and its dominant traits to the grid and utility computing, issues such antivirus service on the cloud has been arose to the high priorities investigations. In this paper we are proposing a method to implement an antivirus service on a private cloud which let the users to scan a target file with the software that is deployed on the server and not on the user.**

**Keywords: cloudAV, SaaS, antivirus engines, VPC, cloud malware protection, cloud computing, anti-virus as a service.**

1. **INTRODUCTION**

Cloud application services or "[Software as a Service](http://en.wikipedia.org/wiki/Software_as_a_Service) (SaaS)" deliver software as a service over the Internet, eliminating the need to install and run the application on the customer's own computers and simplifying maintenance and support. In order to develop the security of internet contents and perform an effective threat management solution that make the world safe for business and customers to exchange digital information, we need to employ a dominant security system. Antivirus software is one of the most widely used tools for detecting and stopping malicious and unwanted files.

Antivirus software is one of the most frequently used devices for detecting and avoiding hateful and annoying files.

Most popular anti-virus programs are not very useful against new viruses, even those that use non-signature-based methods that should discover new viruses. The reason for this is that the virus designers test their new viruses on the main anti-virus applications to make sure that they are not detected before releasing them into the wild some new viruses, specially ransom ware, they use polymorphic code to avoid detection by virus scanners that’s why detecting hateful software has become a more and more demanding problem. While a single antivirus engine may be able to detect many types of malware, 0-day threats and other obfuscated attacks [23], [17] can frequently avoid a single engine. We argue that the executable analysis service presently provided by host-based antivirus software can be more capably and successfully provided as an in-cloud network service. Instead of running difficult analysis software on every end host, we propose that each end host run a lightweight process to obtain executables entering a system, send them to a network service for analysis, and then run or quarantine them based on a threat report returned by the network service. This cloud-based antivirus has several benefits.

* Cloud-based antivirus products use agent software on the protected endpoint that is much lighter than the installed elements of customary antivirus programs.
* reduced dependence on users
* easy PC deployments
* centralized management
* Better detection of malicious software: Antivirus engines have complementary detection powers and a mixture of many different engines can develop the overall recognition of annoying software. This model enables identification of unwanted and unnecessary software by several, varied detection engines in parallel, a technique we name N-version protection.
* Omitting the influence of antivirus vulnerabilities: By moving the complexity of antivirus engines to the network service and dividing the engines within virtualized environments, our cloud deletes the impact of the numerous vulnerabilities present in antivirus engines that may be leveraged by an attacker to compromise a host.
* previous detection of beforehand infected hosts: When signature updates are received, previously analyzed files can be re-scanned, allowing the detection of annoying software and identification of hosts that have been polluted by them.
* Improved forensics capabilities: Information about what hosts accessed what files provides an unbelievably rich database of information for forensics and interruption analysis. Such information provides temporal relationships between file access events on the same or different hosts.
* enhanced deploy ability and management: Moving detection off the host and into the network notably simplifies host software enabling use on a wider range of platforms and enabling administrators to centrally control signatures and impose file access policies.

Along with these benefits, it is important that cloud-based antivirus products thoroughly protect Cloud Systems. The comparison of cloud antivirus solutions to traditional antivirus products now shows that users are benefiting from the use of cloud-based antivirus products.

When using a cloud antivirus product, a small client piece of software runs on each desktop and its connection is made at the central monitoring server in the Cloud. The main operations of antivirus processing and protection take place in the Cloud. The updates to the virus signatures are automatic as long as there is an Internet connection. Infections are tracked at the central server's console and can be viewed from a Web browser.

In this paper we propose an antivirus called McAfee as a service that can be provided by cloud. We want to use windows server as our operation system in this research and also we use Visual studio .NET as an environment to connect between our interfaces used in .NET to our service.

1. **RELATED WORKS**

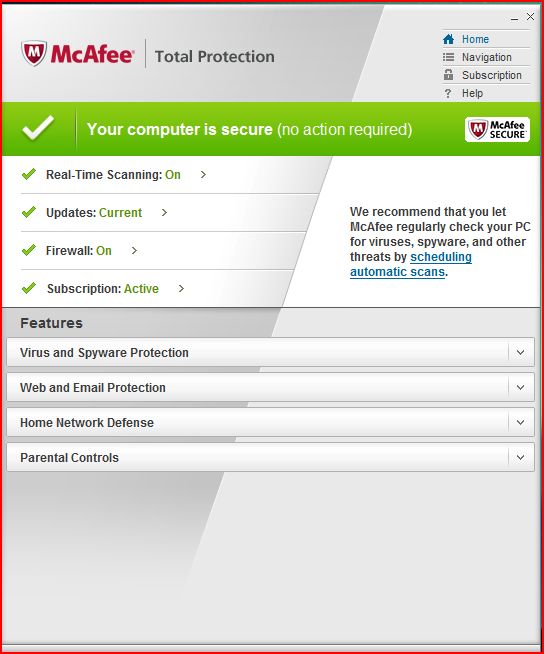
Due to, the benefits that we mentioned and the fast pace growth of cloud usage and popularity among the enterprises and businesses, the services on cloud became more and more important. In field of cloud security, detection of malware, defend the unwanted executable and antivirus services on cloud have been considered by the researchers and many of them proposed new methods and techniques to the implementation of such these services. Here in this part we will review some pervious investigations in this field and their pro and cons.

“John Oberheide” and his research team claimed that the executable analysis currently provided by host based antivirus software can be more efficiently and effectively provided as an in-cloud network service. Instead of running complex analysis software on every end host, it is suggested that each end host run a lightweight process to acquire executable entering a system, send them into the network for analysis, and then run or quarantine them based on a threat report returned by the network service. An executable analysis service run inside an enterprise network or by a service provider could integrate antivirus software, behavioral simulation, and other analysis engines from multiple vendors providing better detection of malware and simplify client software enabling deployment on a broader range of devices. This idea has been constructed by a prototype composed of a Windows based host agent and an in-cloud analysis service and evaluate it using a diverse dataset of 5066 unique malicious executable. By correlating information between multiple detection engines, over 98% detection coverage of the malicious executable were provided by deploying such this system with eight antivirus engines and two behavioral engines compared to a 54% to 86% detection rate using the latest commercial antivirus products.[31]

In another investigation a new model has been proposed for malware detection on end hosts based by serving clients with an antivirus as a service on cloud. In this technique malware and unwanted software are detected by multiple, heterogeneous detection engines in parallel, and a technique we term ‘N-version protection’. By This model author achieve several important benefits including better detection of malicious software, enhanced forensics capabilities, retrospective detection, and improved deployability and management. To explore this idea researcher construct and deploy a production quality in-cloud antivirus system called CloudAV[17]. CloudAV includes a lightweight, cross-platform host agent and a network service with ten antivirus engines and two behavioral detection engines. Then evaluate the performance, scalability, and efficacy of the system using data from a real-world deployment lasting more than six months and a database of 7220 malware samples covering a one year period. Using this dataset we find that CloudAV provides 35% better detection coverage against recent threats compared to a single antivirus engine and a 98% detection rate across the full dataset. We show that the average length of time to detect new threats by an antivirus engine is 48 days and that retrospective detection can greatly minimize the impact of this delay. Finally, we relate two case studies demonstrating how the forensics capabilities of CloudAV were used by operators during the deployment.

Antivirus software and services are used in order to detect and remove viruses, malwares, worms and Trojans. In order to prevent computers from getting viruses in a network such as clouds we have to use anti-virus software. In this work we want to secure our cloud (our virtual private cloud) and protect it against the viruses. Traditional anti-virus software is not suitable for cloud. So we have to use cloud-based anti-viruses. There are some advantages and also some disadvantages for using cloud-based anti-viruses. for example by using cloud-based ones we cannot be sure that each user actives it’s firewall or updates it’s anti-virus software or not. Additionally, there are some advantages and effectiveness of using cloud-based antivirus software .For this approach we can use the SaaS (Software as a Service) model to develop software, and use the software as a service in cloud. Related to our work we can deploy an anti-virus software as a service through internet to make sure the users which are used the cloud are secure and they can use the distributed software as well as their personal anti-virus. There are three famous cloud-based antivirus products:

* McAfee Total Protection Service v5.0.0
* Trend Micro TRVProtect v8 SP1
* Panda Cloud Office Protection v5.04.01

****

* 1. **McAfee** Total Protection Service

McAfee Security-as-a-Service solutions [16] are designed to provide organizations with a comprehensive set of security products built in a Software-as-a-Service (SaaS) model. This strategy takes advantage of our core strength in threat prevention, a diverse SaaS portfolio, and industry-leading McAfee Global Threat Intelligence™, (McAfee GTI™) powered by McAfee Labs™. McAfee Security-as-a-Service solutions are available over the Internet, managed by McAfee, and provided on a subscription basis. With cloud-based security, you reduce your capital investment, eliminate on-site administration, and reallocate IT resources to projects better aligned with your initiatives. And with McAfee Security-as-a-Service solutions, you get immediate, up-to-the-minute threat protection to ensure that your data, systems, and networks are instantly and always secure. What’s being bottom line for you? Peace of mind with lower TCO (Total Cost of Ownership) and less effort.

In comparison between other antiviruses McAfee is very powerful. In order to use this service we have to download the agent and the install it. There are some optional settings to change. Some of its particular characteristics are listed and explained as follow:

1. **Instantly accessible and always on:**

McAfee Security-as-a-Service solutions are instantly accessible and always on. Within minutes, you secure your organization and maximize the value of your software. That’s the beauty of the SaaS model, delivered by the world’s leading security vendor, McAfee. There’s no lag time while you order and set up servers, train staff, and deploy software on every machine or endpoint.

1. **Continuously Updated with Minimal Effort:**

McAfee Security SaaS solutions are updated continuously, without interruption to your users, and requiring minimal administrative effort by your IT staff. These fast updates keep your desktops, servers,

and network proactively protected against ever-evolving security threats in real time. Only McAfee products are backed by McAfee Global Threat Intelligence, which correlates data from a team of 350 researchers, more than 100 million data collection points, and 22,000 customers around the world. It’s like having a team of leading security experts standing outside your door every moment of the day and night.

1. **Comprehensive Security Solutions Built on Rich SaaS Experience:**

With more than a decade of experience and maturity in providing security SaaS solutions, the McAfee portfolio offers comprehensive protection and reliability, geared toward today’s agile and cost-conscious organizations. McAfee offers the most diverse set of Security SaaS solutions available from a single vendor, covering ***email****,* ***endpoint, vulnerability scanning****,* and ***web security*** with reporting and management, all hosted on the McAfee infrastructure.

We can also scan the PC. The test machine with Metasploit triggered more than 2,000 alarms with this scanner. Scan operation have to set manually. When the scan operation completed the result will be emailed to your email address.

* 1. **Trend Micro TRVProtect v8.0 SP1**

Designed for Small and Medium-Sized organizations having between two and 300 Windows-based computers, the TRVProtect [4] managed antivirus service offers you corporate level antivirus & anti spyware protection without the need for the infrastructure or in-house technical knowledge.

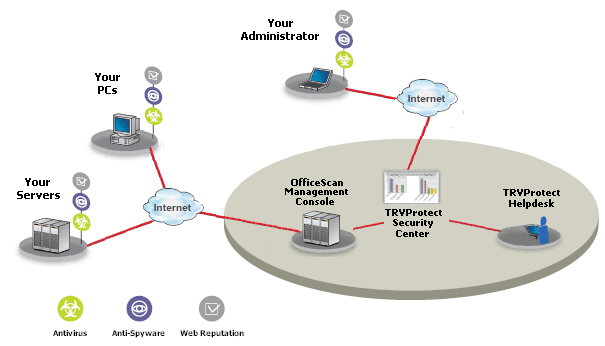
* + 1. **Technically Speaking**

We provide you with a preconfigured OfficeScan installation file with. Simply install the client software on your PCs, servers and laptops and that’s all you have to do! Once protected with our system, you will never need to go back to the computer; simply install and forget! We make all configuration changes and upgrades as part of the service

Once installed, OfficeScan remains in contact with our management consoles on the Internet. Increment an l updates come direct from Trend Micro’s global ‘Active Update’ network. So wherever in the world your computers are located, their protection is always monitored and up-to-date. Virus, spyware and update logs are sent to our consoles allowing you to monitor all your computers from a single point.

No need to create risky incoming firewall rule; all communications are made from your computers to TM consoles. The OfficeScan client is in no way a “backdoor” or any other security risk to your computers. The Security Center web portal allows you to view virus, spyware and update details about your protected computers using the reporting hierarchy of your choice. Email alerts ensure that no virus detections go unnoticed and unactioned! All configuration changes are made centrally without needing to visit the client computers.

As you register activation key will be generated to use for each desktops, [TRVProtect](http://www.trvprotect.com/) will manage the scans by desktop user interface but it doesn’t have a lot of information in the web console which is worked with the IE.

****

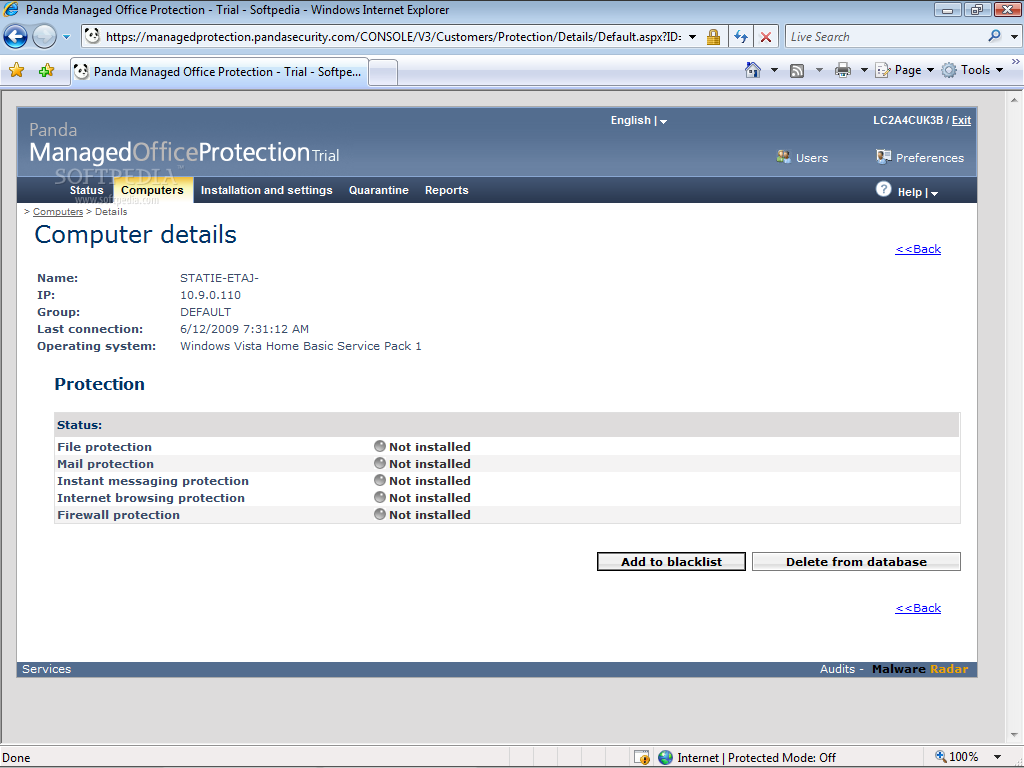
****

With the unique Security Centre web portal that this company provides, you can monitor virus, spyware and update statistics covering all your protected computers from a single point. Monitor your virus and spyware logs. TRV Security constantly monitors to alert you of any serious problems on your computers. Since TRVProtect takes up just 50 MB of RAM of desktops it is the most less consuming of storage among the three software which are discussed in this report [18].

* 1. **Panda Cloud Office Protection v5.04.01**

Panda Cloud Office Protection [28] is a cutting edge endpoint security solution that offers cloud-based antimalware and firewall protection. The solution forms part of Panda Security’s innovative Panda Cloud Protection suite. It is an easy-to-use, secure solution providing constant, robust, real-time protection for workstations, laptops and servers. Based on the concept of software as a service (SaaS), it harnesses the power of Collective Intelligence’s knowledge base from the cloud which delivers maximum real-time protection against known and unknown threats. Maximum security gives companies the peace of mind to focus on their core business and forget about the costs, complexities and troubles associated with traditional security products.Panda security is a free antivirus service but for some features of this product we have to pay. These products need to be downloaded and installed before use. There are three paid products which are used for endpoint protection, hosted email protection and loss prevention, are respectively suitable for desktop firewall, antivirus and antispyware and browser access controls.

In order to use the Web console you have to download a windows installer package for each desktop and when you run this you have to update the signature files.

****

You can see the scan results on the desktop, and also at the Web console. The “Panda software “have at least eight different agents that takes up 60 MB of RAM.

Panda is the most flexible among these three services that offers “scheduled scan” in client-server products. we cannot say that one of the above cloud-based products is better than the others, and none of them is really complete. Obviously the cloud is not a safe place still to protect your PCs, but each of these producers tries to improve the company’s products.

1. **Cloud Anti-Virus**

Typically the **''**Cloud Antivirus**''** can be extended in two ways [7]:

* One in which the user clicks on an email which includes a link that will install the protection agent.
* The other way is where administrator can push the installation to workstations choosing workstations by name, IP address, and IP range or by domain. They are similar to other free antivirus but hosted in cloud.
* Some Advantages of Cloud-antivirus:

Works with 32bits Operating Systems as well as for 32bit processes under 64bit systems.

* Self-protection of the AV processes and configurations.
* Automatic upgrades to new engine versions and new features automatically and transparently.
* Improved offline protection. Default deactivation of Windows Auto run.
* Ability to run alongside other AVs and Anti-Spyware**.** Can now be run alongside other security tools and scanners.
* Full scan option**.** Added option to run a full PC scan easily.
* Optimized installation background scan by using adaptive low-priority scans.
* Improved scanning progress information by showing when a large compressed file is being scanned to avoid the perception that the stuck is stuck.

**V.METHODOLOGY**

In this work we used the “Microsoft’s solution for private cloud” [29], which is a windows-based virtual cloud. It built on Windows Server 2008 R2 Hyper-V platform and it organized by “Windows Server Directory” framework. It virtualized on Hyper –V and for applications we used the “System Centre”. Windows Server 2008 R2 is the infrastructure for us to build the private cloud. We use the “built-in Hyper-V” hypervisor in order to virtualize the servers, clients and their applications. [20]

There are some advantages in using the Microsoft Virtual Cloud that listed below:

* It helps us to use the application service management for business.
* It gives us the opportunity to build a hybrid cloud model.
* It helps us to customize and control the resources of cloud.
* It increases the flexibility of cloud computing.
* It works with various kinds of platforms such as VMware, Hyper-V and also Citrix

**What is Hyper-V?**

Hyper-V is a part of Windows Server which is used to virtualization and transition to cloud. It has so many benefits that some of them is listed below:

* By using the Windows Server 2008 R2 you can find the solution for virtualization scenarios.
* Generating server confirmation.
* You can have “Dynamic data centre”.
* Hyper-V provides us more flexibility with some features such as live migration and cluster shared for storage flexibility [5].

**Build a Virtual Private Cloud (VPC) by using Microsoft Technologies**

In our project we want to set up the Private Cloud environment by using current release versions of Microsoft products. We will download the TRIAL free versions of all we need from Microsoft website.

After the installation and configuration of private cloud completed, you will be able to use the “System Centre Virtual Machine Manager” and the” SCVMM Self Service Portal 2.0” to build and manage a Private Cloud.

**In our project we will need:**

* ***A Host Machine*** which these component have to be installed on it:

Windows Server 2008 R2 + SP1 + all post SP1 Updates

*And on this “*Windows Server 2008” *we have to install:*

* Active Directory Domain Services
* DNS Server,
* Hyper-V,
* Web Server (IIS)
* *Software such as :* SQL Server 2008 R2 x64, System Centre Virtual Machine Manager 2008 R2 Server
* Components and Administrator Console, SCVMM Self Service Portal 2.0
* ***Guest VM’s –*** when this installation completed, you be able to create as much as guest VM’s as you like.

**Software Requirements:**

In our project we will need to download trial versions of software for testing, they will work for 180 days since we install the operating system. We can download tem from these links.

* + [Windows Server 2008 R2 with SP1 Trial](http://technet.microsoft.com/en-us/evalcenter/ee175713.aspx?lc=1033)
  + [System Centre Virtual Machine Manager 2008 R2 with SP1 Trial](http://technet.microsoft.com/en-us/evalcenter/cc793138.aspx)
  + [Microsoft SQL Server 2008 R2 Trial](http://technet.microsoft.com/en-us/evalcenter/ee315247) (64bit version) as we can see in figure6.
  + [Microsoft System Centre Virtual machine Manager Self-Service Portal 2.0 with SP1](http://www.microsoft.com/download/en/details.aspx?id=26701).it shows in figure 7.

**Install SQL Server 2008 R2**

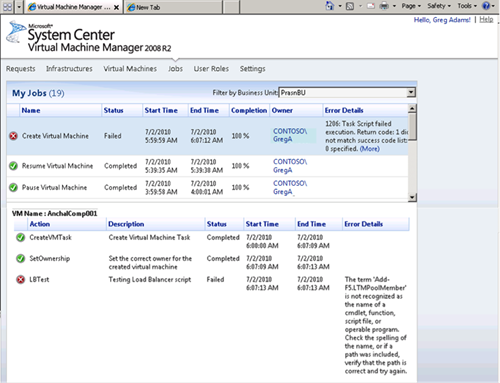
SQL Server 2008 R2 is suitable for storing the information of configuration for “System Centre Virtual Machine Manager” and the “SCVMM Self-Service Portal”. [11]

**The System Centre Virtual Machine Manager R2 + SP1 (VMM Administrator Console)**

By installing the Virtual machine manager Administrator console, Now we have the interface which is used for virtualization infrastructure.

**The SCVMM Self-Service Portal 2.0 with SP1**

This is one of the important components of private cloud. By using this feature, administrators can create resources such as storage, networks and load balancers. Administrators can manage the resources and make them available per client requests.

****

After all we have a Virtual Private Network that we can implement the antivirus on it.

In order to provide the interaction between our application (software as a service) and user/customer we need an API (an interface).Our goal is to build this API with .NET programming so the user as a client can connect through the API to virtual private cloud as a server to scan the files or to be sure that the cloud is secure. The target users of this work will be the organizations, companies or any community which want to reduce the cost, increase the efficiency and better use of resources in their working environment. In our project we are eager to implement the service for users convenient. They won’t need to install high weight antivirus programs on their systems.

**VI. What is cloud anti-virus service?**

Cloud antivirus software as a service consists of two main parts that work together:

* Client
* Web service components

The client side is a small program running on your local computer that scans the system for malware, viruses and etc. Full locally installed antivirus applications are used a large amount of computer resources, but cloud antivirus clients require only a small amount of resources such as processing power.

The Web service part of the cloud antivirus is software which is running on one or more servers somewhere on the Internet. The Web service (SaaS) handles most of the data processing so your local computer doesn't have to process and/store massive amounts of virus information.

Here are some of the advantages of cloud antivirus in comparison with traditional ones:

* With cloud antivirus web service you have access to the most recent updated data about malware. There's no need to update your antivirus software periodically to be sure of the fully protection from the latest threats.
* The cloud antivirus client side is a small program, and it requires little processing power.
* You can use the free versions of cloud antivirus software. Also you can purchase for additional utilities and support by upgrading your software with lower prices in comparison with locally installed ones.
* Cloud antivirus splits its tasks between your computer (i.e. a client application) and Web servers that can be everywhere on the Internet. Since cloud antivirus can leverage resources from different parts of the Internet to better defend your computer against malware. For each cloud antivirus product such as McAfee, these resources come together to form a database of malware data.
* One of the most important advantages of cloud antivirus is that how quickly they can make that data available to you. Rather than downloading some big patch for your antivirus software every few weeks.

The McAfee® Cloud Security, a key component of the Security Connected framework, helps businesses safely and confidently takes advantage of cloud computing by improving and applying their own security practices and policies to data moving to and from the cloud. This suite secures email, web, and identity authentication traffic, leveraging McAfee Global Threat Intelligence™ for real-time protection against the latest threats.

**VII. The security as a service advantages:**

With a security SaaS approach, a service provider takes the responsibility for maintenance of the technology investment. In exchange for a regular, recurring fee user will benefit in many cases.

Antivirus vendors now offer products and services that provide inline support for hosted email and messaging systems. They also update their antivirus products as a service. And nowadays, some antivirus vendors have expand their services even further, with antivirus and anti-Trojan coverage to the users as a “data loss prevention (DLP)” SaaS to complete the message filtration. “Hosted encryption service” that can complement DLP, expand the range of data security which is provided as a service.

**7.1. User view:**

**Cost:** as a user you don’t need to purchase antivirus software and install it, instead of you can rent this service from cloud and scan your file in cloud, you can do this action very easy by opening one webpage and upload you file inside it and then scan your file.

**Hardware efficiency:** Also in this method user doesn’t need to install new antivirus software in personal computer, thus user don’t need have specific configuration, for example for install some software you need specific size of memory, hard disk, processor speed and so on, it means that cloud antivirus independent from hardware.

**Maintenance:** In cloud antivirus responsibility of management and maintenance of software such as update antivirus is by cloud provider and as a user you can only use this software and don’t need to update and manage software.

McAfee Security-as-a-Service solutions which are exist through the internet, managed by McAfee and provided on a subscription basis. By running security as a cloud-based solution, customer/user can:

* Cut your capital investment
* Remove onsite administration
* Reallocate IT resources to projects better configuration to your initiatives
* You get quick and up-to-the-minute threat protection to ensure your data, systems, and networks are immediately and always secure.
* Easy on the budget ,McAfee Security-as-a-Service solutions deliver peace of mind
* User doesn’t need hardware to install.
* Continuously updated with minimal effort

**Disadvantage of this service for user:**

**Speed:** You need fast internet connection and Rather than software installed in computer the speed is low, because for scan and check one file u need to upload it in webpage and wait to receive answer from cloud provider, and this task for some user that have low speed connection to internet is very bad and time consuming, for example if you want to scan huge number of file this manner takes long time and not suitable.

**Not real time:** This method is not real time and don’t have ability to check virus file when it arrive to computer but you need to choose and upload that file in webpage cloud service and then check it and maybe computer damage in during this process.

**7.1.1. Security issues:**

* **Compute in the cloud with more confidence**: Overcome common cloud computing security concerns and compliance obstacles by extending corporate security and policies to apply to cloud traffic.
* **Secure all your critical data**: Protect, identify, and classify all critical data while it moves between the enterprise and the cloud — email, web, and authentication traffic.
* **Operate with more efficiency and flexibility**: Reduce IT drag by combining data loss prevention, email, web, and identity and access management under a single, modular-based platform. Deploy in a variety of form-factors, including on-premise appliances, cloud, or a hybrid of both.
* **Protect the sensitive information in your databases**: Take advantage of the increased scalability, flexibility, availability, and the lower costs offered by the cloud, while carefully monitoring data to make sure it is protected. Meet the requirements of compliance regulations with McAfee Database Activity Monitoring.
* **Security for Web 2.0 traffic:** SaaS Web Protection uses complex technologies to analyze the nature, Tendency, and behaviour of an active content of web page. This deep analysis proactively protects against unknown malware, mixed threats, phishing sites, and targeted attacks.

**7.2. Service provider view:**

**Cost:** As a cloud service provider you don’t need to produce and copy number of software and you don’t need to use cd od dvd for writing software and also the delivery and selling task cost is reduce by this method, you only place one copy of software on your server and all your customer connect use to it.

**Maintenance:** Maintenance and management task is reduced by only having one copy of software in server and as a service provider you need to manage only one copy of it.

Easy adoption is the greatest benefit in large Enterprises to extent their access to capability. In many cases, user doesn’t need to deploy; they simply enable the service. That is similar to adding inline web proxies for safe browsing services.

When the service is activated, following maintenance becomes the responsibility of the service provider. Capital investment and high maintenance costs that were unpredictable before shift from a customer which is under contract. The cost of new security technologies is reduced or eliminate and they become more predictable.

* One of the advantages of the security SaaS model is that some hosted parts can be accessed from virtually anywhere through internet. ***For example***: “Hosted message filtration services” can be used as email security in an organization, enables the access to the service regardless of location.
* Better allocation of security resources to where it’s most needed is one major benefit for a technology vendor which uses this approach.
* The scalability enhances the value of this approach to the service providers. because, the customer "rents" not only the provider's technology, but also the capabilities of its data centres as well.
* Businesses are either forgoing using cloud computing or are building private clouds to minimize the cost and efficiency benefits.
* There’s no time delay while you order and set up servers, train staff, and deploy software on every machine or endpoint.
* This SaaS is updated steady, without interruption to your users and demanding minimal executive effort by your IT staff. These fast updates keep your desktops, servers, and network proactively protected against ever-evolving security threats in real time.
* Service provider:
* For the enterprise, by reaching the security SaaS the providers reach expanding of the security management and reduce a lot of their complexities that this will result in free up resources for more strategic priorities. For the small and medium-sized business, it will increase the higher level of capability.
* The other advantages of security SaaS are Scalability and immediate adaptability for highly distributed Enterprises. "Adding capability solely without adding more security engineers to use it is an absolute benefit for provider," says Ed Bellis. When the service provider conforms to new or Appearance issues such as recently disclosed vulnerabilities or threats, it is that much less for enterprise security teams to handle.
* A SaaS model can suggest "enterprise-class" security capability to the smallest organization and also it can do at the predictable cost of a sharing, because the provider can distribute its costs to many customers. For the SMB, this does more than get rid of preventive initial investment costs and ongoing maintenance responsibilities; it gives them gain to technologies that might otherwise be beyond their reach.

**Implementation:**

We implemented a website that shows Antivirus as service. We can upload any files to this website as a client and the server that has McAfee Antivirus as a service scan our file whether it detects any viruses or not. McAfee scan our file and send the result to the client.

We implemented our website with C#.net and Asp.Net.

**Prerequisite for running this website:**

1-Visual studio .net 2008 or 2010

2-IIS (Internet Information Services)

The source code:

using System;

using System.Collections.Generic;

using System.Diagnostics;

using System.IO;

using System.Linq;

using System.Threading;

using System.Web;

using System.Web.UI;

using System.Web.UI.WebControls;

public partial class \_Default : System.Web.UI.Page

{

protected void Button1\_Click(object sender, EventArgs e)

{

if (scanfile())

{

Label1.Visible = true;

Label1.Text= "No Virus Detected";

}

else

{

Label1.Visible = true;

Label1.Text = "Virus Detected and File Can Not Be Uploaded";

}

}

public bool scanfile()

{

bool IsValid = true;

try

{

//do av check here

Process myProcess = new Process();

FileUpload1.SaveAs(Server.MapPath(@"~\upload\") + FileUpload1.FileName);

//address of command line virus scan exe

myProcess.StartInfo.FileName = @"C:\Program Files (x86)\McAfee\VirusScan Enterprise\scan32.exe";

string path = '"' + "" + Server.MapPath(@"~\upload\") + "" + FileUpload1.FileName + "" + '"';

string report = '"' + "" + Server.MapPath(@"~\upload\Report.txt") + "" + '"';

string myprocarg = "/SCAN=" + path + " /REPORT=" + report;

myProcess.StartInfo.Arguments = myprocarg;

myProcess.StartInfo.CreateNoWindow = true;

myProcess.Start();

myProcess.WaitForExit(); //wait for the scan to complete

//add some time for report to be written to file

int j = 0;

int y = 0;

for (j = 0; j <= 1000000; j++)

{

y = y + 1;

}

Thread.Sleep(10000);

//Get a StreamReader class that can be used to read the file

StreamReader objStreamReader = default(StreamReader);

objStreamReader = File.OpenText(Server.MapPath(@"~\upload\Report.txt"));

String reportVerbose = objStreamReader.ReadToEnd().Trim();

if (reportVerbose.Length > 0 && !reportVerbose.Contains("Found infections : 0"))

{

IsValid = false;

File.Delete(Server.MapPath(@"~\upload\") + "" + FileUpload1.FileName);

}

objStreamReader.Close();

if (IsValid)

{

try

{

if (!Directory.Exists(Server.MapPath("~/upload/")))

Directory.CreateDirectory(Server.MapPath("~/upload/"));

if (

!File.Exists(

Server.MapPath(@"~\upload\" +

System.IO.Path.GetFileName(FileUpload1.PostedFile.FileName))))

{

FileUpload1.SaveAs(Server.MapPath(@"~\DataFiles\") + FileUpload1.FileName);

}

else

{

try

{

File.Delete(

Server.MapPath(@"~\upload\" +

System.IO.Path.GetFileName(FileUpload1.PostedFile.FileName)));

FileUpload1.SaveAs(Server.MapPath(@"~\DataFiles\") + FileUpload1.FileName);

}

catch (System.IO.IOException)

{

}

}

}

catch (System.IO.IOException)

{

}

}

else

{

}

myProcess.Close();

}

catch (System.IO.IOException)

{

}

return IsValid;

}

}

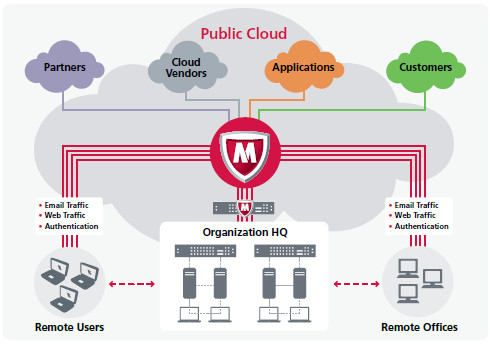






# SaaS (Software as a Service) Hosting:

Software providers delivered their software solutions by installing and supporting them on their clients' internal computers and networks before. Nowadays, software providers are receiving more requests to deliver their Software as a Service (SaaS) in a hosted environment so customers can avoid the *expense and complexity of running these systems internally*. Besides, software vendors prefer to focus on developing software, not managing infrastructure.   
  
In our experiment we have to host our web application on a domain and after that we have to design an API for our client side, in order to make connection between client and server, or we can design a light software with low memory or processor usage, it can be a software written by any programming languages or an URL or IP address of the host, where our main program/software is installed. We should install the antivirus which we used in our project to provide an Antivirus software as service (Which we use the C# for our implementation).The McAfee antivirus is used in our experiment. We can build a virtual private cloud as we mentioned before by using the “Microsoft’s solution for private cloud”, which is a windows-based virtual cloud. It built on Windows Server 2008 R2 Hyper-V platform and it organized by “Windows Server Directory” framework. It virtualized on Hyper –V and for applications we used the “System Centre”. Windows Server 2008 R2 is the infrastructure for us to build the private cloud. We use the “built-in Hyper-V” hypervisor in order to virtualize the servers, clients and their applications. We tried to find a free cloud to host our web service there or a free domain that provide the antivirus for us but we couldn’t. We hope to buy a domain and host our web service there in a cloud-based hosting service to illustrate the distributed concept which is the goal of cloud computing.



McAfee protects key cloud traffic channels

1. **Expected Results**

Cloud Antivirus is a service that uses just a small amount of Ram and hard disk. The expected result from the different detection engines is the combination of definition of whether a file is safe to open, accessible, executable or quarantined. Several variables can influence this process. For example if the detector fails, it may never return the result.

Cloud Antivirus is based on a cloud security solution that can be installed and managed from anywhere through a web console. Inasmuch as it is a hosted service, it doesn’t require infrastructure investment. We normally have switches to representative our security management to expert service providers. So it is basically more about management of Antivirus in any organization that goes in the cloud. However we have options to control the updates, profiles and levels of security from a cloud based control panel [7], [17].

Cloud Antivirus is a service not software and so has following advantages: We get advantage of low track and up to date packages."Cloud Antivirus" will scan all our files through the internet and run the tests on their own server, in this way neither it won’t disturb any of our computer activity nor will it slow down our computer. Another benefit of cloud antivirus is that, it automatically updates the virus definitions in the cloud instead of updating traditional antivirus software normally and then scans our files to see if it is contaminated with any of the new virus. The next one is that you don’t need installation on your personal computer. The important thing is that has capability to update without user intermediation. Also you can access to your account from anywhere easily. Another advantage is that reduces bandwidth which uses as large number of workstations looks for updates in traditional software. We will have Less false positive (i.e. a file as a virus when it is not a virus).It requires fewer resources from users' computers. Cloud antivirus reduces the on-disk track, in-memory usage, CPU required to update your computer, and bandwidth costs. **It allows for quicker innovation** and alsoit only uses a small amount of ram and hard disk.

**IX. FUTURE WORK**

With any advance in science and technology there will always be critics and people opposed to change. In this post we have a list of disadvantages of cloud-based antivirus which we resolve them in future. Let us review them [30]:

A cloud-based antivirus needs to check everything against the cloud. So it takes more time.

It is an invasion of privacy. I do not want my files & documents to leave my computer.

**This is one of the most common misconceptions, maybe due to some weak implementations of cloud-scanning by some vendors. At least we have to implement cloud scanning to Portable Executable (PE) files, so your Word/Excel documents, etc. are not checked against the cloud.**

Cloud-based antivirus do not protect while offline.

To resolve this issue we have to design an antivirus that **has a local cached copy of the Collective Intelligence cloud servers. This local cache is tasked with detecting (even while not connected to the Internet) malware that is in the wild, non-PE malware and other threats.**

**X. REFRENCES**

[1] G. C. Blog, “Cloud Servers Locations Blog Benefits Of Cloud-Based Antivirus Products Benefits Of Cloud-Based Antivirus Products,” 2011.

[2] I. T. E. Pa, “Service Definition for Private Cloud.”

[3] B. Peng, B. Cui, and X. Li, “Implementation Issues of A Cloud Computing Platform,” *Design*, pp. 1-8.

[4] T. Management, “Trend micro inc.,” *Security*, 1988.

[5] E. Overview, “An Enterprise Private Cloud Architecture and Implementation Roadmap,” *Computing*, no. June, 2010.

[6] C. Articles, C. Directory, and G. Blogging, “SaaS Introduction with Examples ­ Cloud Service RECENT ARTICLES,” *Computing*, 2010.

[7] P. Posts and Y. Favorite, “LINUX SECTION WINDOWS SECTION SEMINAR TOPICS,” *Current*, 2011.

[8] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian, “Virtualized In-Cloud Security Services for Mobile Devices,” *Electrical Engineering*.

[9] “Software-as-a-Service Security Solutions,” *Micro*, pp. 1-1, 2010.

[10] K. Ruan, P. J. Carthy, P. T. Kechadi, and M. Crosbie, “Cloud forensics : An overview,” *InformationWeek*, no. 2009.

[11] T. Wood, “The Case for Enterprise-Ready Virtual Private Clouds University of Massachusetts Amherst.”

[12] T. Problem, “ONDotNet.com: Service-Oriented Architecture Explained Página 1 de 3,” *Architecture*, pp. 2003-2005, 2004.

[13] U. Guide, “Amazon Virtual Private Cloud,” 2011.

[14] S. Add, “How Does a Cloud Antivirus Work ?,” *Portal*.

[15] J. Oberheide, E. Cooke, and F. Jahanian, “Rethinking Antivirus : Executable Analysis in the Network Cloud,” *October*.

[16] S. Brief, E. Delivered, I. Accessible, and A. On, “McAfee Security-as-a-Service,” *Security*, no. 2009, pp. 2009-2011, 2011.

[17] J. Oberheide, E. Cooke, and F. Jahanian, “CloudAV : N-Version Antivirus in the Network Cloud.”

[18] “Service Provider Market Growth Why Partner with Trend Micro ? Service Provider Partner Benefits,” *Micro*, 1988.

[10] C. S. Provider, “VMware vCloud Implementation Example.”

[20] M. a Vouk, “Cloud computing — Issues, research and implementations,” *ITI 2008 - 30th International Conference on Information Technology Interfaces*, pp. 31-40, Jun. 2008.

[21] Y. Ye, “Combining File Content and File Relations for Cloud Based Malware Detection,” *Security*, pp. 222-230, 2011.

[22] P. Cloud, “If you thought that protecting your computers meant buying new servers and wasting valuable time on complex con guration tasks, then think again. We o er you a security solution which is easy to install and manage , and requires no new infrastructure . ,” *Computer Operations*.

[23] P. Royal, M. Halpin, D. Dagon, R. Edmonds, and W. Lee, “PolyUnpack: Automating the Hidden-Code Extraction of Unpack-Executing Malware,” *2006 22nd Annual Computer Security Applications Conference (ACSAC’06)*, pp. 289-300, Dec. 2006.

[24] C. E. Avis, “How to build a FREE Cloud using Technologies …. SBS Security SQL Systems How to build a FREE,” *Archives*, 2011.

[25] P. Summary, “The CloudAV TM Architecture : N-Version Antivirus in the Network Cloud Project Summary :”

[26] X. Zheng, T. Li, and H. Yang, “A Novel Cloud-based Worm Propagation Model,” *Journal Of Computational Information Systems*, vol. 4, pp. 1082-1091, 2011.

[27] C. A. Martínez and G. I. Echeverri, “Malware Detection based on Cloud Computing integrating Intrusion Ontology representation,” *Context*.

[28] Cloud, P. (n.d.). “PANDA Cloud Office Protection” *Computer Operations*

[29] Packs, S., & Manager, V. M. (2008). How to build a FREE Private Cloud using Microsoft Technologies Architecture : Software Requirements : *Portal*.

[30] Bustamante, P. (2009). “Arguments against cloud-based antivirus”

[31] Oberheide, J., Veeraraghavan, K., Cooke, E., Flinn, J., & Jahanian, F. (n.d.). “Virtualized In-Cloud Security Services for Mobile Devices” Electrical *Engineering*

[32] Scott Crawford, CISSP, CISM, “An IT industry analyst and consulting firm “ is managing research director of the security and risk management practice with Enterprise Management Associates (EMA),

|  |
| --- |
|  |
|  |  |
|  | | | | |
| http://media.techtarget.com/informationsecurity/images/spacer.gif | |  |  |  |
|  |