Software as a secured and maintained engineering good using cloud

G. Ganesh Srim, Bhargava Ganti
Assistant Professor
Computer Science Department, Gayatri
Vidya Parishad, College of engineering(A)
Visakapatnam-530048, India

S. S. K. Sandeep Ray
Assistant Professor
Computer Science Department, Srinivasa Institute
of Engineering and technology Cheyyeru East
Godavari District, India

Abstract—People are very much aware of the fact that the software that is being installed in a computer system is secured in the presence of security software like antivirus. But the same people waver about its security in the cloud. In our paper we address this issue as a prime implication. As a matter of fact we have different categories of cloud like public, private, protect and community clouds which are custom build with lots of investments made on that. An important factor that is being embodied in the cloud is the security. As crore’s of rupees are invested towards the deployment of firewalls to protect the cloud. As a part of our paper we attempt to bring certain issues related to cloud like the cost of maintenance along with the security in the cloud into lime light also emphasize the advantages and disadvantages associated with our focused area.

Keywords—Cloud Software Security, Maintenance of Software’s in Cloud.

I. CLOUD EXTENDED TO SOFTWARE
A major concern about software is that, it differs in functionality from computer to computer. As this Competitive world requires fast processing, the cost of the computers and their maintenance is getting rapidly increased. So hiring a cloud as a package with intended specifications as services and hosting the software on it leads to cost efficient and enhanced processing capabilities. Let us consider an example: Running a Data server at own house needs a firewall that merely costs Rs.1,00,000 and a server with minimum specifications costs around Rs.75,000. In addition its maintenance costs are considerably high. An efficient solution to this problem can be provided by cloud as it comes inclusive of firewalls and its pay by use costs are relatively low.

II. CLOUD
Cloud Computing can be defined as the novel style of computing where virtualized resources are provided as services on internet which are dynamically scalable. Cloud computing represents a different way to architect and remotely manage computing resources. It refers to both application delivered as a service over the internet and system software in the datacenters that provide those services. The data centre hardware and software are collectively called cloud.

2.1 Cloud Types:
A common distinction is Public Clouds, Private Clouds, Hybrid Clouds and Community Clouds

2.1.1 Public Cloud:
A public cloud, or external cloud, is the most common form of cloud computing, in which services are made available to the general public in a pay-as-you-go manner. Customers – individual users or enterprises – access these services over the internet from a third-party provider who may share computing resources with many customers. The public cloud model is widely accepted and adopted by many enterprises because, the leading public cloud vendors as Amazon, Microsoft and Google, have equipped their infrastructure with a vast amount of data centers, enabling users to freely scale and shrink their rented resources with low cost and little management burden. Security and data governance are the main concern with this approach.

2.1.2 Private Cloud:
A Private Cloud, or internal cloud, is used when the cloud infrastructure, proprietary network or data Center, is operated solely for a business or organization, and serves customers within the business fire-wall. Most of the private clouds are large company or government departments who prefer to keep their data in a more controlled and secure environment.

2.1.3 Hybrid Cloud:
A composition of the two types (private and public) is called a Hybrid Cloud, where a private cloud is able to maintain high services availability by scaling up their system with externally provisioned resources from a public cloud when there are rapid workload fluctuations or hardware failures. In the Hybrid cloud, an enterprise can keep their critical data and applications within their firewall, while hosting the less critical ones on a public cloud.
2.1.4 Community Cloud:
The idea of a Community Cloud is derived from the Grid Computing and Volunteer Computing paradigms. In a community cloud, several enterprises with similar requirements can share their infrastructures, thus increasing their scale while sharing the cost. Another form of community cloud may be established by creating a virtual data center from virtual machines instances deployed on underutilized users machines.

2.2 CLOUD SERVICES:
A Cloud is essentially a class of systems that deliver IT resources to remote users as a service. The resources encompass hardware, programming environments and applications. The services provided through cloud systems can be classified into Infrastructure as a service (IaaS), Platform as a Service (PaaS) and Software as a service (SaaS).

2.2.1 Infrastructure as a Service:
The IaaS is categorized into:
1) Computation as a Service (CaaS), in which virtual machine based servers are rented and charged per hour based on the virtual machine capacity – mainly CPU and RAM size, features of the virtual machine, OS and deployed software.
2) Data as a Service (DaaS), in which unlimited storage space is used to store the user’s data regardless of its type, charged per GB for data size and data transfer.

Amazon has provided a popular universal and comprehensive solution to Cloud Computing, called the Amazon Elastic Compute Cloud (EC2). EC2 provides many useful features for customers, including a mature and inexpensive billing system able to charge for computing at a very fine-grained level (memory usage, CPU usage, data transfer, etc.), deployment between multiple locations, elastic IP addresses, connection to a customer’s existing infrastructure through a Virtual Private Network, monitoring services by Amazon Cloud Watch, and elastic load balancing. EC2 has deployed such fine granularity and precision that it has become a benchmark and model in cloud computing.

GoGrid also provides Hybrid Hosting, which is a distinguishing feature. Many applications simply don’t run well in a pure multi-tenant server environment. Databases perform better on a dedicated server where they don’t have to compete for input/output resources, and the situation is similar with web server applications. GoGrid provides these special applications with dedicated servers that also have high security assurance.

2.2.2 Platform as a Service:
Platform as a Service (PaaS) cloud systems provide an execution environment that application services can run on. The environment is not just a pre-installed operating system but is also integrated with a programming-language-level platform, which users can be used to develop and build applications for the platform.

Microsoft’s cloud strategy is to construct a cloud platform that users can move their applications to in a seamless way, and ensure its managed resources are accessible to both cloud services and on-premises applications. To achieve this, Microsoft introduced the Windows Azure Platform (WAP), which is composed of a cloud operating system named Windows Azure, and a set of supporting services. Windows Azure is the main part of the WAP. It employs virtual machines as its runtime environments.

2.2.3 Software as a Service:
Software-as-a-Service (SaaS) is based on licensing software use on demand, which is already installed and running on a cloud platform. These on-demand applications may have been developed and deployed on the PaaS or IaaS layer of a cloud platform. SaaS replaces traditional software usage with a Subscribe/Rent model, reducing the user’s physical equipment deployment and management costs. The SaaS clouds may also allow users to compose existing services to meet their requirements. This section presents some SaaS clouds and applications.

III. FIREWALLS
There are two different categorised firewalls in nature:

3.1 Hardware Firewall:
A hardware firewall is a standalone product such as a broadband router (a picture of a broadband router is shown in figure 1.) It allows connected computers to transfer data between each other and access the internet. The hardware firewall or router uses packet filtering as the method to transfer data. It compares the header of the packets and determines the destination and source addresses. It then compares the addresses to rules and based on these rules the packets are either transferred or dropped.

Figure 1: “Design the Firewall System“
Another method of transferring data is SPI, state full packet inspection. This is where the router determines the origin of the packet and transfers or drops it based on the computer behind the routers request. There is a slight downfall with the router, when information is transferred form connected computers, i.e. two computers connected to the router, the router does not check the contents of the data. It assumes that the data being transferred is safe and completes the transfer. Therefore if a connected computer already has a virus or Trojan it will pass on the virus or Trojan to the other connected computers. The main advantage of a hardware firewall is that it protects all connected computers from harmful material from the internet. It is effective and easy to use. To use a router just plug in your computer(s) to the router using proper cables, the firewall is ready in use with none, or very minimal configuration required. A hardware firewall is an easy and safe way to protect a computer or network of computers from the internet.

3.2. Software Firewall:
Software firewalls are program based applications that run on a computer. They work by monitoring all open ports on a computer and checking all the information that is received on them. Each monitored port is specifically dedication to each program that has access to the internet, so the software firewall, is configured to contain a list of applications available to access the internet on certain ports. Therefore, if the allowed application is using a specified port, the software firewall will check the contents coming in on that port and pass it through to the computer if acceptable. If an application attempting to access information that is not allowed/configured to from the internet, the firewall will block all incoming/outgoing information and notify the user that that program is trying to access the internet, thus allowing the user to determine if the application is safe to have access to the internet. A software firewall can protect a computer and notify the user of any activities trying to access the personal computer from anywhere outside the computer. The software firewall gives a lot of control over the information passing through the computer and can be a very effective way for an advanced user to protect its computer from the outside. If the software firewall is configured properly it can be very effective, but it can also be difficult to configure. For local area networks, software firewalls must be installed on each machine on the network and configured separately. Depending on the size of the network and the amount of configuration needed, it can be very cumbersome and difficult to maintain a software firewall on a network.

3.3. Differences between H/W and S/W Firewalls:
There is no main difference between hardware and software firewalls in the end they both do the same task. They both act as barriers between the internet and the computer and they both help protect them from anything harmful that can harm the computer from the outside connection. The choice between choosing the firewall is purely preference, but there should be some thought when choosing. The best and most minimum that one should do to protect a computer is to have a hardware firewall in place. The ease of setting up and the range of protection for various numbers of computers is an obvious choice. To improve the protection, adding a software firewall can pretty much eliminate most if not all incoming or outgoing harmful materials from the internet. Although more configurations are required with a software firewall, there is more flexibility and control for the user. In the ideal situation the best would be to have both hardware and software firewalls they both will give the good protection from the internet.

IV. REQUIREMENTS FOR DEPLOYING AN APPLICATION OVER PUBLIC CLOUD

4.0.1. Licensing: 
Application is made up of many components which are associated with some license agreements. Analysis should be made about the effects of those license agreements on the deployment of application on cloud. Applications which are designed licensed for CPU, when we deploy it on the cloud increases the load by exciding the CPU license limit.

4.0.2. Processing requirements and memory locks: 
Application should be designed to work on the parallel architectures, because of the dynamic scalability of cloud. Multi-threaded code which allows process to split in to small chunks suits for the cloud environment. A single threaded application cannot take the real advantage of clouds distributed nature.

4.0.3. Bandwidth requirements: 
Because a public cloud is accessed via the Internet, bandwidth is significantly limited when compared to a private cloud. Given the public cloud’s bandwidth limitation, applications that have moderate client bandwidth requirements should only be considered.

4.0.4 Communication protocol: 
The cloud is based on the Internet Protocol (IP), so for an application to be considered, it must use IP as its communication mechanism. While there are many protocols that can be run over IP, the use of Transport Control Protocol (TCP) is preferred.

4.0.5 Data security: 
The application will need to provide security at the data storage, processing and transmission stages. Three critical components of this are:
- Data in transit needs to be protected either at the application or the transmission level.
Data at rest must be protected by the application. The application must provide a mechanism to protect the data stored in the cloud. Encrypting data at rest is the best option at this time, and a future technical tip will delve into the specifics of this area.

Servers to server communications are typically forgotten because they currently exist within the data Center.

V. APPLICATION DEPLOYMENT

In this section we present an example how the combination of virtualization and on of self-service facilitate application deployment in this example we consider a two-tier Web application deployment using cloud.

4.1.1 Steps for deployment

The following steps comprise the deployment of the application:

- A load balancer, Web server, and database server appliances should be selected from a library of preconfigured virtual machine images.
- Configuring each component to make a custom image should be made. Load balancer is configured accordingly; web server should be populated with the static contents by uploading them to the storage cloud whereas the database servers are populated with the dynamic content of the site.
- The developer then feeds the custom code in to the new architecture making components meet their specific requirements.
- The developer chooses a pattern that takes the images for each layer and deploys them, handling networking, security, and scalability issues.

The secure, high-availability Web application is up and running. When the application needs to be updated, the virtual machine images can be updated, copied across the development chain, and the entire infrastructure can be redeployed. In this example, a standard set of components can be used to quickly deploy an application. With this model, enterprise business needs can be met quickly, without the need for the time-consuming, manual purchase, installation, cabling, and configuration of servers, storage, and network infrastructure.

VI. IMPLEMENTATION RESULTS IN THE SECURITY OF PHYSICAL INSTALLED APPLICATION AND CLOUD HOSTED APPLICATION

The Major factors that differ in both are:

- Portability
- Data Security
- Data Recoverability
- Standardisation
- Cost
- Maintenance

Now the above are the factors that differ the working of an application either in standalone physical system or a cloud hosted system.

<table>
<thead>
<tr>
<th>Factor</th>
<th>CLOUD</th>
<th>Physical System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portability</td>
<td>Every where</td>
<td>Not Possible</td>
</tr>
<tr>
<td>Data Security</td>
<td>High</td>
<td>Considerable</td>
</tr>
<tr>
<td>Data Recoverability</td>
<td>High</td>
<td>Average</td>
</tr>
<tr>
<td>Cost</td>
<td>Depends</td>
<td>Depends</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Less</td>
<td>Less</td>
</tr>
<tr>
<td>Standardisation</td>
<td>Yes</td>
<td>May not</td>
</tr>
</tbody>
</table>

The recoverability issues were so good in cloud rather than in a physical system. Data recovery in a cloud is easier than a physical system.

VI. CONCLUSION

Cloud computing is a very flexible paradigm for delivering computational power. It means many things to many people. For some it means being able to set up a new start-up company knowing that initial resources will be inexpensive but a sudden increase in demand from users won’t make the company a victim of its own success, as has happened in some cases in the past where servers have been unable to cope with demand, and the company loses clients as they become unhappy with poor response times.

The Cloud allows automatic backup at every state of change hence the restoration of data is easier rather than in physical system the Cloud application allows two way Virtualisation firewalls.

REFERENCES

- Deploying an Application on the cloud by N.Rama Ganga Charan