



Cloud Computing Security Using Keys & Encryption

Sonia^[1], Monika Monga^[2], Ashish Raj^[3]

^[1]Associate Professor, Department of Information Technology, MIMIT, Malout, Punjab, India.

^[2]Lecturer, Department of Computer Science and Engineering, MIMIT, Malout, Punjab, India.

^[3]Research Scholar, Department of Computer Science and Engineering, MIMIT, Malout, Punjab, India.

Abstract: The security in the cloud is a concern nowadays and security professionals are still finding same hardware means to make cloud computing more secure. The installation of the ESX5.0, Vsphere, vCenter Server, Porticor-VPD in server hardware is successful in building the platform & allows the creation and deployment of many virtual servers. These servers have operating systems and applications, which are permanently used and stores valuable information, by making an encryption key & Master key. This research paper aimed to show how possible it is to use a cloud encryption & cloud key management system in the cloud environment.

Keywords: Cloud Computing, Network Security, Virtualization, Encryption.

I. Introduction

Service providers build their own data centers to serve their customers. A data centre is a place where companies keep their physical hardware. It is usually composed of many servers, routers and switches interconnected together. Usually data center requires a lot of space, consuming resources and energy. Redundant links exist between those allowing the companies to use their services via the Internet or private IP-based networks at anytime and anywhere. Thus customers do not need to know where their data are being kept. However adding more and more equipment to their rack system saturates the data centre and consumes energy. Looking ahead there will be an increase in the management costs and resource utilization in the near future. To Overcome those limitations, the virtualization technology was introduced.

Cloud Security: Internal vs. External

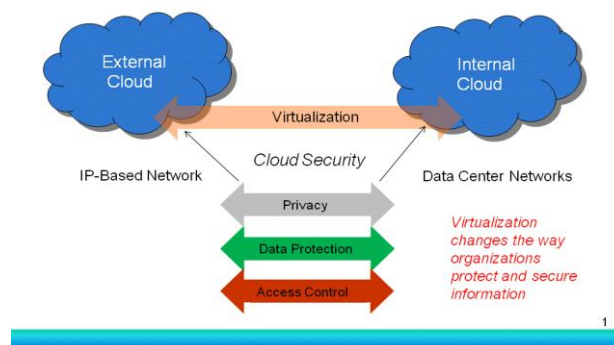


Fig. 1: Internal & External Cloud Security

Now many virtual servers can be run in the while using small re- sources. Applications and software are developed and deployed through the web inter- face in this virtual data center. Cloud computing is the ability to use applications and software on the Internet which stores and protect the data while providing a service [1]. It improves energy efficiency and lows management costs. Customers will be billed only when the virtual resources dedicated to them are being used. The network is running and needs to be maintained in a case of an incident to satisfy the availability of the services. One can think at this step, installing a cloud key management system will be a good idea. The cloud encryption & key management system will monitor the activities of the virtual servers and all the applications, which are built in those appliances. Whether in use or at rest, both the data and the encryption keys must be handled and deployed correctly. An effective encryption solution must address every stage in the lifecycle.

II. Cloud Computing

Like the meteorological phenomena from which it takes its name, cloud computing cannot be easily defined. There are many definitions, which share the same common denominator: the Internet. Cloud computing is a way to use the Internet in the daily life from a single machine or single room, using all the tools installed on

computers. It is also the ability to use shared computing resources with local servers handling applications. With cloud computing users do not worry about the location and the storage of their data. They just start using the services anywhere and at anytime. The main driver of this technology is virtualization (Hypervisor) and virtual appliance [3].

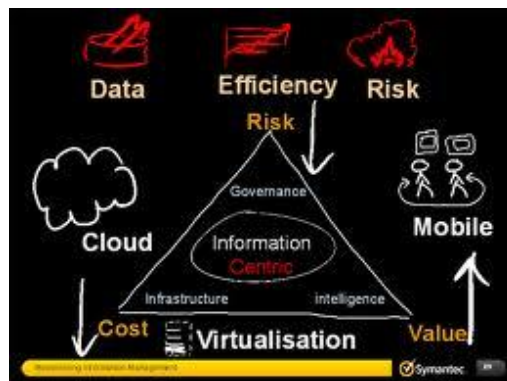


Fig. 2: Role of Virtualization

Virtualization provides a means to separate the physical hardware and the operating system and applications by simulating software [4]. The software called hypervisor is uploaded inside the computer. That software in turn also uploads files that define a virtual computer, a virtual machine. A virtual appliance is an application that is grouped together with all the components that it needs in order to run with an operating system. The virtualization of computers and operating systems hides the physical characteristics of computers to the users. The hypervisor is a part of virtualization, which allows many virtual operating systems to run on the same physical machine instantaneously [5].

In the same server hardware, one was able to install many instances of virtual servers, which are connected together via the virtual switch. This architecture allows the creation of a virtual data center with the same functionalities as a real rack system environment.

III. Delivery model

Software as a Service (SaaS)

In software as a Service, an application is hosted by the service provider and accessed via the World Wide Web by the client [6]. An easy way to see the idea behind software as a service is to think about the web-based service offered by companies like Google (Google doc) and Microsoft (Microsoft Office 365). The vendor hosts all the programs and data in a central location, providing end users with access to the data and software through the World Wide Web. Software as a service offers the biggest cost savings over installed software by eliminating the need for enterprises to install and maintain hardware. The vendors have meticulous security audits. Software as a service removes the need for an organization to handle the installation, setup and daily maintenance of its application. In this model, the resources are outsourced and accessed at anytime.

Platform as a Service (Paas)

Platform as a service is the delivery and deployment of computer applications over the Internet with the consideration that all the parties needed in the development process are already obtained [7]. An organization usually needs to worry about building its own virtual machine images, configuring the storage and network. Using Paas, network, storage and virtual machine images are already pre-built by the provider. Additionally the provider monitors the virtual machine for failure and initiate auto-recovery when needed. An example of platform as a service is Ubuntu 10.10 Server in Amazon elastic cloud computing (EC2) in which a user is given an Internet protocol (IP) address and access the server in the cloud infrastructure using the secure shell protocol (SSH)[13]. Platform as a service provides the entire infrastructure needed to run applications over the Internet with security and scalability. Developers are now able to code, test to fix bugs, deploy and maintain applications in the same computing environment.

Infrastructure as a Service (IaaS)

Data infrastructure is moving towards a utility model just like electricity and telephone bill. Infrastructure as a service allows organizations to outsource the equipment used to support operations including storage, server, hardware and network component. A client purchases or rents computing power or disk space, which they can access through their mobile, or desktop PC. The provider hosts the client's web site while monitoring the availability of the service. Rather than purchasing software, a server, data centre space or network equipment, clients buy those resources as a fully outsourced services. Platform offered on top of the Infrastructure as a service can deliver rapid provisioning of applications allowing greater agility and reducing time for developers. It should scale to avoid limitations. A typical example of IaaS is Gogrid. [8]

Security as a Service

Cloud computing providers use security as a Service model to deliver real time security protection. The increased use of the Internet has raised the need to protect companies' assets against malware or data theft. Organizations and enterprises can then bring outsourcing to cyber security in order to secure their data, content and communication. Security as a service shifts all the security inspection, enforcement and management processes from the customer's location to the cloud provider. The antivirus in this case is provided to the clients through the web browser. Using security as a Service, enterprises are certain to have the vulnerabilities in their system discovered and mitigated on time. A typical example is Zscale cloud services.[9]. Bitdefender Beta has a version called BitDefender Safego which acts like an application in the Facebook profile and checks for any infected link in the wall.[10]. Security as a service provides encryption & key management system to protect the data with a master key which is very confidential. A typical example is Porticor key management system.

IV. Security Benefits

Data Leakage

The biggest benefit is the centralization of data. Organizations have an issue with asset protection, in no small part because of data being stored in numerous places, like laptops and the desktop. Thick clients are apt to download files and maintain them on the hard drive, and there are plenty of laptops out there with files. Using thin clients creates a better chance for centralized data storage. As such, there's less chance for data leakage. Centralization also provides the opportunity for better monitoring. That data is in one place makes it easier to check in on your data and see that everything is okay.

Offloading Work

Another security benefit isn't so much a technology, but the fact that you don't have to do it yourself. It's up to the cloud provider to provide adequate security. After all, can your organization afford 24/7 IT security staffing? The fact of the matter is that your cloud provider might offer more security features than you had before. The fact that so many clients are paying allows cloud providers to have beefier security, simply because of the economy of scale involved. That is, there are many paying clients so the provider is able to do more, because there is more money in the pot. Plus it's to the provider's benefit to offer more, because they want to get a good reputation.

Logging

Logging is also improved. It's something that, in-house, usually gets the short end of the stick. But in the virtualized world of cloud computing, providers can add as much memory as they need to extend logging[12].

Forensics

If there is a breach, the cloud provider can respond to the incident with less downtime than if you had to investigate the breach locally. It is easy to build a forensic server online, and it costs almost nothing until it comes into use. If there is a problem, the virtual machine can be cloned for easy offline analysis. Further, many companies don't have a dedicated in-house incident response team. If there is a problem, IT staff have to quickly figure out their new job of taking the server down, quickly investigating, and getting it back online for minimal production downtime.

Development

Even more good news is that security vendors aren't in the dark about this whole cloud thing. They are actively developing products that can apply to virtual machines and the cloud. Security vendors also have a unique opportunity in the cloud. Since it's new ground, there are new opportunities for the vendors who are open-minded enough to imagine them.

Auditing

As an IT professional, you already know the headache of securing your own local network. But when you send your data to the cloud, a whole new set of issues arise. This is largely because your data is being stored on someone else's equipment.

Compliance

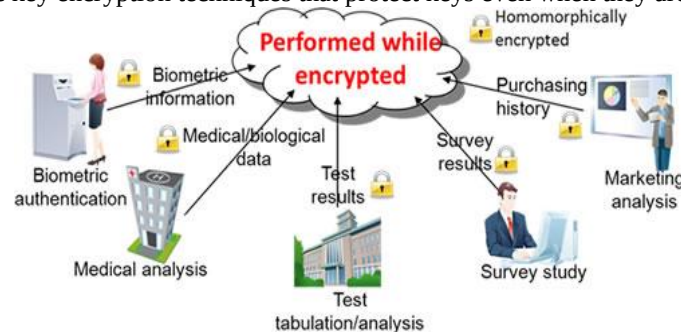
The same security issues that your organization deals with are the sorts of issues that SaaS providers face—securing the network, hardware issues, applications, and data. But compliance adds another level of headache. Regulations like Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLBA), and HIPAA, and industry standards like the Payment Card Industry Data Security Standard (PCI DSS) make things particularly challenging. Prior to SaaS, compliance could be managed by a few tasks: Identify users and access privileges, sensitive data, where it's located, how it is encrypted. Document this for auditors and regulators. SaaS makes these steps even more complicated. If you store compliance-sensitive data with an SaaS provider, it is difficult to know where the data is being stored. It could be on the provider's equipment, or it could even be on the equipment of one of the provider's partners.

V. Building cloud encryption key

This implementation examines the risks to data in the cloud and introduces the Virtual Private Data system, which combines state of the art encryption with patented key management to protect critical data in public,

private and hybrid cloud environments. Most of the companies uses 3 core technologies to deliver trust in the cloud:

- Robust, standards-based data encryption with a convenient, fast and simple management interface
- Cloud-ready key management using patented Split-Key Encryption
- Homomorphic key encryption techniques that protect keys even when they are in use



Each of these plays a vital role in ensuring that your data is safe and that your encryption keys are protected, both when in storage and when in use in the cloud. Together, they make Virtual Private Data the only solution that offers the convenience of encryption and key management in virtualized environments, without sacrificing trust.

1. Firstly we build a cloud server through ESX 5.0 server with the help of installing VSphere client[14].
2. ESX server will give an IP address & login with a unique username & password .The IP is connected to the VSphere client.
3. Launch the VMware VSphere client & deploy a new OVF template [2].
4. After deploying the OVF template , click on the newly created virtual appliance & power it on.
5. Next, click edit settings to add a virtual disk & we will create two 1 GB virtual disks.
6. We recommend making the disk independent so encrypted data will be saved regardless of the virtual machine.
7. Make a note of the IP address & fire up your web browser.
8. Type “https://” followed by the virtual appliance IP address.
9. You will be redirected to key management service & complete the registration. Create a new project & after initialization creates a DNS name for your appliance.
10. After this you will get a master key. Most important keep your master key in a safe place.

VI. The Challenges of Securing Data at Rest in Private and Public Clouds

Data encryption is one of the most important methods of protecting data at rest in the cloud and as a result, the number of solutions available – from open source APIs to proprietary turnkey projects – has mushroomed. In order to select the most effective solution for your needs, it’s important to understand the primary challenges of encrypting data in the cloud [11].

- **Managing the encryption process:** For complex applications with large amounts of data, the most time-consuming aspect of data encryption is management: deployment, set-up, adding and removing disks, etc. An effective encryption solution can reduce the time required from each of these tasks from hours to minutes.
- **Securing the data lifecycle:** Whether in use or at rest, both the data and the encryption keys must be handled and deployed correctly. An effective encryption solution must address every stage in the lifecycle.
- **Delivering high performance:** To ensure that the quality of service for your business applications meets expectations, the encryption solution must offer very high performance.
- **Ensuring trust in the cloud:** The problem with hosting key management in the cloud is one of trust. For both security and compliance reasons, you cannot afford to allow a third party to manage your keys. In order to benefit from the convenience and low cost of cloud-based key management, you need a sophisticated solution that leaves the root of trust in your hands alone.
- **Storing and managing the encryption keys:** Every time the application accesses the data store. It needs to use encryption keys. There is generally one key per disk or data store and all of them must be managed on a key management server. Hosting a key management server in the data center is expensive, undermining the cost benefits of cloud projects. On the other hand, storing keys in the cloud raises the very important issue of trust.
- **Protecting the keys from theft when they are in use:** Encryption keys are vulnerable at two points – when in storage, and while in use. A truly effective key management solution will be able to protect the keys at both times.

VII. Conclusion

Cloud computing is being the emerging technology in use today. It is cost-effective because a user is charged only for what he or she uses. There are three different types of cloud computing: private cloud, public cloud and hybrid cloud. Those platforms are used to provide services to companies in a way that there is no need to download any additional software. A browser and an Internet connection are enough. Therefore permanent threat and attack facing this evolving technology exists. As a solution to mitigate those attacks a cloud key encryption management system was built in this project. Data encryption is critical to protecting the security of data at rest in the cloud. But when it comes to the cloud, encrypting the data is only the beginning – managing and protecting the encryption keys effectively is vital. An effective data encryption solution must include: Robust, fast, yet easy to use data encryption, Reliable, cloud-based key management that is cost-effective, but trustworthy, Key encryption technologies to protect your encryption keys as well as your data – both in storage and in use.

References

- [1] Introduction to cloud computing architecture [online]. Sun Microsystems USA: Santa Clara: Sun Microsystems 2009. <http://www.scribd.com/doc/17274860/Introduction-to-Cloud-Computing-Architecture>.
- [2] PorticorVPD-v2,18rc4 <http://www.Portico.com/register/?source='side bar'>
- [3] Application architecture for cloud computing [online]. Path: Raleigh NC http://www.rpath.com/corp/images/stories/white_papers/WP_ArchitectureForCloudComputing.pdf cloud computing pdf.
- [4] Virtualization is it right for you? [online]. LAD enterprisesInc <http://www.ladenterprizes.com/pdf/Virtualization.pdf>.
- [5] Hypervisor [online]. Techtarget. <http://www.searchservervirtualization.Techtarget.com/definition/hypervisor>.
- [6] What is SaaS and What are its advantages? [online]. Metaquote Software <http://www.teamwox.com/en/teamwox/tutorials/71>.
- [7] Cloud computing [online]. Cloud computing Asia: 2010. <http://www.cloudcomputinglive.com/asia/platform-as-a-service.html>.
- [8] GoGrid[online]: Gogrid. . <http://www.gogrid.com>.
- [9] Cloud computing-Evaluating security as a service [online]. Quinstreet Inc:2011. www.cioupdate.com/trends/article.php
- [10] Bitdefender Safego [online]. Bit defender <http://www.bitdefender.com/media/html/facebook/safego/>.
- [11] Cloud key management whitepaper <http://www.porticor.com/porticor-key-management-white-paper>.
- [12] Anthony T. Velte, Toby J. Velte, Ph.D., Robert Elsenpeter, “cloud computing- A Practical Approach”.
- [13] Amazon Elastic Compute Cloud (EC2), <http://www.amazon.com/ec2/>.
- [14] ESX and vCenter Server Installation guide [online]. VMware Inc, USA: Palo Alto :2009-2010 http://www.vmware.com/pdf/vsphere4/r41/vsp_41_esx_vc_installation_guide.pdf.