Mr. Shailesh V. Ugale, Prof. S. J.Karale / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 2,Mar-Apr 2012, pp.1002-1005

Azure Framework, way to Resolve Security Issues In Cloud Computing

Mr. Shailesh V. Ugale* Prof. S. J.Karale**
*(M. Tech. Computer Science Engineering Yashwantrao Chavan College of Engineering, Nagpur, India
**(Computer Technology Department Yashwantrao Chavan college of Engineering, Nagpur, India

Abstract—
The Cloud computing concept offers dynamically scalable resources provisioned as a service over the Internet. Economic benefits are the main driver for the Cloud, since it promises the reduction of capital expenditure and operational expenditure. In order for this to become reality, however, there are still some challenges to be solved. Amongst these are security issues.In this project we identified some security issues between different servers in cloud computing like malicious attack and fingerprinting etc. We resolve these issues by proposing a security framework like dummy client, which send particular number of request to control server and then analyzing the response to identify, affected server and prevent them to take further request from control server in cloud computing environment.

I. Introduction

The economic case for cloud computing has gained widespread acceptance. Cloud computing providers can build large datacenters at low cost due to their expertise in organizing and provisioning computational resources. The economies of scale increase revenue for cloud providers and lower costs for cloud users. The US National Institute of Standards and Technology (NIST) defines cloud as follows :"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can berapidly Provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics three delivery models, and four deployment models." [1].

Cloud computing is not a new technology but rather a new delivery model for information and services using existing technologies. It uses the internet infrastructure to allow communication between client side and server side services/applications (Weiss, 2007). Cloud service providers (CSP's) offer cloud platforms for their customers to use and create their web services, much like internet service providers offer costumers high speed broadband to access the internet. CSPs and ISPs both offer services. The cloud provides a layer of abstraction between the computing resources and the low level architecture involved. The customers do not own the actual physical infrastructure but merely pay a subscription fee and the cloud service provider grants them access to the clouds resources and infrastructure. A key concept is that the customers can reduce expenditure on resources like software licenses, hardware and other services (e.g. email) as they can

obtain all these things from one source, the cloud services provider. Recent studies have found that disciplined companies achieved on average an 18% reduction in their IT budget from cloud computing and a 16% reduction in data center power costs. In this paper, we propose a comprehensive security framework for multi server communication in cloud computing environments. We present the security issues and policy in cloud computing environment.

Ii About Cloud Computing

To understand the importance of cloud computing and its adoption, we must understand its principal characteristics, its delivery and deployment models, how customers use these services, and how to safe- guard them. The five key characteristics of cloud computing include on-demand self-service, ubiquitous network access, location-independent resource pooling, rapid elasticity, and measured service, all of which are geared toward using clouds seamlessly and transparently. *Rapid elasticity* lets us quickly scale up (or down) resources. *Measured services* are primarily de- rived from business model properties and indicate that cloud service providers control and optimize the use of computing resources through automated resource allocation, load balancing, and metering tools.Applications running on or being developed for cloud computing platforms pose various security and privacy challenges depending on the underlying de- livery and deployment models.The three key cloud delivery models are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). In IaaS, the cloud provider supplies a set of virtualized infrastructural components such as virtual machines (VMs) and storage on which customers can build and run applications. The application will eventually reside on the VM and the virtual operating system. Issues such as trusting the VM image, hardening hosts, and securing inter-host communication are critical areas in IaaS.PaaS enables programming environments to access and utilize additional application building blocks. Such programming environments have a visible impact on the application architecture, such as constraints on which services the application can request from an OS. For example, a PaaS environment might limit access to well-defined parts of the file system, thus requiring a fine-grained authorization service.

Finally, in SaaS, the cloud providers enable and provide application software as on-demand services. Because clients acquire and use software components from different providers, crucial issues include secure- ly composing them and ensuring that information handled by these composed services is well protected.

Cloud deployment models include public, private, community, and hybrid clouds. Public clouds are external or publicly available cloud environments that are accessible to multiple tenants, whereas private clouds are typically tailored environments with dedicated virtualized resources for particular organizations. Similarly, community clouds are tailored for particular groups of customers

Iiicloud Computing Architecture

Cloud computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service. Architecture styles define families of software systems in terms of patterns for characterizing how architecture components interact [7]. The types of architecture components that exists, and constraints on how they may be combined (fig:1). The Key Business Architectural Principles includes Business Alignment, Cost Optimization, Compliance with Laws and Regulations, Minimize Cost. Technology Independence, Adherence to Standards, Common Development Methodology, Loosely coupled Interfaces, Implement Information Lifecycle Management, Regulatory and Legal Compliance, and Enforce of Data Privacy.

1. Business Architecture

Cloud offers unprecedented control in allocating resources dynamically to meet the changing needs of a business. Application performance metrics and SLAs mustbe carefully documented and monitored for an effective cloud deployment.

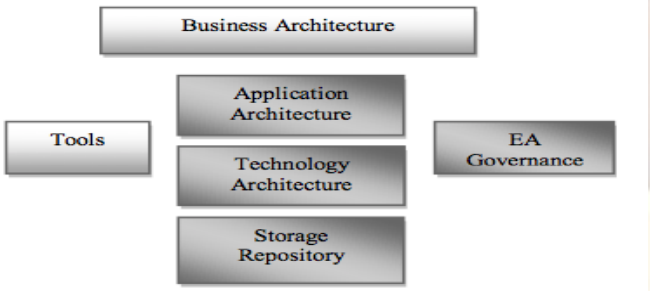

Figure 1. Cloud Computing Architecture

*2.***Application Architecture**

Application services should abstract resource allocation and avoid the tight binding of its resources to invokers of the service. To take advantage of the cloud's scalability capabilities, applications should take advantage of distributed application design and utilize multi-threading wherever possible. Applications should leverage distributed locking, Information Architecture Cloud computing offers the potential to utilize information anywhere in the cloud. This increases the complexity associated with meeting legal and regulatory requirements for sensitive information.

C. Technology Architecture

Implementing Service Oriented Architectures provides the most effective means of leveraging the capabilities of cloud computing. SOAs distributed nature, service encapsulation; defined service level objectives, virtualized interfaces, & adherence to open standards align with Cloud's architectural requirements.

Storage architecture includes the capabilities of the Google file system along with the benefits of a storage area network (SAN). Google file structure can be used in the cloud environment. When used, it uses the disks inside the machines, along with the network to provide a shared file system that is redundant. This can increase the total data processing speed when the data and processing power is spread out efficiently.

Iv. Security Issue and Policy In Cloud Computing Environment

Cloud computing is a new computing model, regardlessof the system's architecture or service's deployment isdifferent from the traditional computing model. Thereforetraditional security policies are not able to respond to theemergence of new cloud computing security issues [8].

A. Security Issue In Cloud Computing Environment

a) Cloud computing can not be clearly defined boundariesto protect the device user, the traditional computing modelcan protected device user by dividing physical and logicalsecurity zones.

b) Service security issues. The cloud service provider controls the data, communications networks, services and other important resource. So when provider'ssecurity is something wrong, how to ensure that the servicecontinue to be used, as well as the confidentiality of userdata is particularly important.

c) Protection for user data. This issue includes location ofuser data stored, the way of data storage, data recovery, dataencryption and data integrity protection.

d) The number of users changes dynamically, as well asuser use the different services, leading the user can not beclassified.

e) In cloud computing model, the cloud service providerhas too large right. However, the user's rights may be difficult to ensure. Therefore, how to balance the rightsbetween the service providers and users becomes a problem.

f) Due to the complexity of cloud computing, and theuser's dynamic changes in cloud computing environment, how to ensure communications among the various subjectsare security and integrity is an important issue to beconsidered.

B. Security Policy In Cloud Computing Environment

In order to solve these problems, the security policy should include the following points:

a) Divided into multiple security domains in the cloudcomputing environment, different security domain operationmust be mutual authentication, each security domaininternal should have main map between global and local.

b) Ensure that the user's connection and communicationssecurity with the SSL, VPN, PPTP, etc. Using license andallowing there are multiple authorizations among user,service owner and agents, to ensure user access to datasecurely.

c) User data security assurance: according to the differentuser's requirements, different data storage protection should be provided. At the same time, the efficiency of data storageshould be improving.

d) Using a series of measure to solve the user dynamic requirements, including a complete single sign-on authentication, proxy, collaborative certification, and certification between security domains.

e) Establishment of third-party monitoring mechanism toensure that operation of cloud computing environment issafe and stable.

f) The computing requested by service requestor, shouldcarry out the safety tests, it can check whether they contain malicious requests to undermine the security rules.

V.Pros And Cons Of Cloud Computing

One of the advantages of cloud computing is it permitsaccessibility to multiple data centers anywhere on the globe.It is more environments friendly [11]. Reducing the numberof hardware components and replacing them with cloudcomputing systems reduces energy costs for runninghardware and cooling as well as reducing carbon dioxideemissions and conserving energy. Moving applications tothe cloud can potentially reduce energy costs for runningand cooling hardware.

The benefits of deploying applications using cloudcomputing include reducing run time and response time,minimizing the risk of deploying physical infrastructure,lowering the cost of entry, and increasing the pace of innovation. The barriers ofcloud computing includes DataSecurity.

Manycustomers don't wish to trusttheir data to "the cloud". So data must be locally retained for regulatory reasons. The other cons are latency since thecloud can be many milliseconds away and it may not besuitable for real-time applications. Moreover the applicationavailability is another drawback they cannot switch fromexisting legacy applications. The major disadvantage ofcloud computing is data security as data has to betransmitted from one end to another.

Vi. Security Framework For The Cloud

In this section, we provide an overview of our proposed security framework for multiserver communication in cloud computing environment and then articulate some approaches to address its security issues. Basically we are designing a security model, which is deal with different security issue betweendifferent servers while communicating with each other in the cloud. There are mainly two security issues, we concentrate on these are malicious server attack and fingerprintingattack. We propose the system which is base on azure framework which provide us a cloud setup on which we create different servers, on these no of servers one is maliciousserver which cannot increase his load count butcontinuously taking request from the control server. Control server distributed each request coming from user with minimum load formula, that is it directed the given request to server having lowestload and because of maliciousserver is under attack he always shows minimum load, therefor he takes all the request from control server and send same reply to user that his request is under process. Another attack is fingerprinting attack. Inthis security framework weidentify theirsignature and by designing different security algorithm .we try to remove these security issues

Vii.Experimental Environment

A. Microsoft azure framework

Azure framework is the best availabletool, which providesus cloud setup on which we carried out the different operation in different server. Azure framework required Microsoft visual studio ultimate 2010 on which we download the Microsoft azure tool, which contain azure emulator, which carried out total creation process of cloud. It creates different server then allocating the different ports for each server to avoid collision. Because of azure we are not required to physically setup cloud, which is very complicated job instead of that using virtualization process these tool create, the cloud emulate the working of the cloud. Azure is Microsoft product there for we must use visual studio, which is also useful tool for properly acquiring azure tool and implementing it

Viii. Conclusion

In this paper, we propose a comprehensive security framework cloud computing environments. The focus of this paper is to understand the structure of cloud and the different security issue cloud computing and propose security framework to resolve the above mention issues.

References

[1] Hassan Takabi and James B. D. Joshi, *"StateMiner: An Efficient Similarity-Based Approach for Optimal Mining of Role Hierarchy", In Proc. of the 15th ACM symposium onaccess control models and technologies (SACMAT10), USA, ACM Press, 2010.*

[2] Cloud Security Alliance Report, *"Security Guidance for Critical Areas of Focus in Cloud Computing V2.1"* (http://cloudsecurityalliance.org/)

[3] Daniele Catteddu, Giles Hogben, (ENISA report) "Cloud Computing:Benefits, risks and recommendations for information(http://www.enisa.europa.eu/act/rm/files/deli

verables/cloud-computingrisk-assessment/at download/fullReport)

[4] Jian Wang Yan Zhao Shuo Jiang Jiajin Le College of Information Science and Technology, Donghua University Shanghai, China *"Providing Privacy Preserving in cloud computing".*

[5] Michael Airburst, Armando Fox, Rean Griffith, Above the cloud: *A Berkeley View of Cloud Computing[R] Technical Report No.UCB/EECS-2009-28.*

[6] C.Kang, Z.WeiMing, *Cloud computing: system Instance and Current Reaserch, Journal of software, 2009.20(5):1337-1347*

[7] Francesco M.A and Gianni F. *"An approach to a cloud Computing network", IEEE, August 2008, pp113-118*

[8] Amazon EC2 Service. http://aws.amazon.com/ec2

[9] Networking, vol. 31, no. 9, pp. 805-822, 1999. [2] Cloud Security Alliance. Security Guidance for [9*] "Critical Areas of Focus in Cloud Computing". April, 2009. http://www.cloudsecurityalliance.org/*

[10] I. Foster, C. Kesselman, G. Tsudik, S. Tuecke. *Security Architecture for Computational Grids. Proc. 5th ACM Conference on Computer.*

[11] M. Tim Jones, Cloud computing with Linux, 10 Sep, 2008. http://www.ibm.com/developerworks/library/cloud computing/

[12] Z.Cheng, L.Bing, Rearch on the Stack Model of Cloud Computing,Microel Ectronics&Computer, 2009.8