17-18 December 2012, ICRTITCS – 2012, TCSC, Mumbai, India
Proceedings published in International Journal of Computer Applications® (IJCA) (0975 – 8887)

Cloud Computing: Security Issues, Mitigation and a Secure Cloud Architecture

Tejaswi Agarwal
School of Computing Science and Engineering
Vellore Institute of Technology-Chennai
Tamil Nadu, India
tejaswi.agarwal2010@vit.ac.in

Amrit Sahoo
Department of Computer Science and Engineering
National Institute of Technology-Trichy
Tamil Nadu, India
amritsahoo@gmail.com

ABSTRACT

Cloud computing, an emerging field in Information technology has changed the perception of infrastructure architectures, software delivery and deployment models. The concept of Cloud computing comes into focus when the basic aspect of information technology is considered which involves a way to increase capacity on the fly without much investment either in hardware or software. In a nutshell, cloud computing could be classified as a term for delivering hosted services, dynamically scalable and shared resources on the internet. Research in this technology has gained tremendous momentum in the past few years since its inception and one of the key research areas is considered to be the security aspects of cloud computing. This paper will classify the three models of cloud computing, some key differentiating aspects between cloud, grid and distributed computing, a comprehensive study on the major security concerns in cloud computing, its mitigation and describe a secure cloud computing framework with an implementation of Single Sign on mechanism on Ubuntu Enterprise Cloud.

GENERAL TERMS
Cloud Computing, Security, Cloud Architecture

KEYWORDS
Cloud Computing, Security, Secure cloud Architecture, internet, security challenges

1. INTRODUCTION

Cloud Computing, a new jargon in computing models which uses a client or any public computer connected to the host for providing business or consumer IT services over the internet. The most widely accepted definition of Cloud Computing given by National Institute of Science and Technology, USA is "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". The services could range from high end data storage and processing to basic software and client email services available on demand. It enables users to access resources online without considerations about location, time or physical and technical maintenance issues of the resources requested [1]. Cloud computing is more scalable, dynamic and fault-tolerant than conventional computing forms and hence has the capability of providing infinite computing resources on demand. As Cloud Computing has advantages for both providers and users, it is developing in an extraordinary pace and predicted to grow and be adopted by a large amount of users in the near future. Cloud computing involves getting services at a much lesser cost to the user, and the maintenance cost is zero as the service provider is responsible for availability.

Cloud computing was developed mainly to have extensive hardware connected to support downtime on multiple devices over a network. The structuring models in cloud computing can be classified into three domains as:

Software-as-a-Service (SaaS): Software as a service is software that is deployed as a hosted service and accessed over the Internet to run behind a firewall in your local area network or personal computer. This is an "on-demand" model deploying patches and upgrades to the application transparently, and delivering access to end users over the Internet through a browser or smart-client application [2].

Platform-as-a-Service (PaaS): PaaS can be defined as a computing platform that allows the creation of web applications quickly and easily and without the complexity of buying and maintaining the software and infrastructure underneath it . PaaS enables the end user to create and maintain software using the libraries and tools of the service provider.

Infrastructure-as-a-Service (IaaS): Infrastructure as a service refers to a facility availed by organisations that offers users the leverage of extra support operations, including storage, hardware, servers and networking components. The resources are owned by the service provider and the client pays on per-use basis.

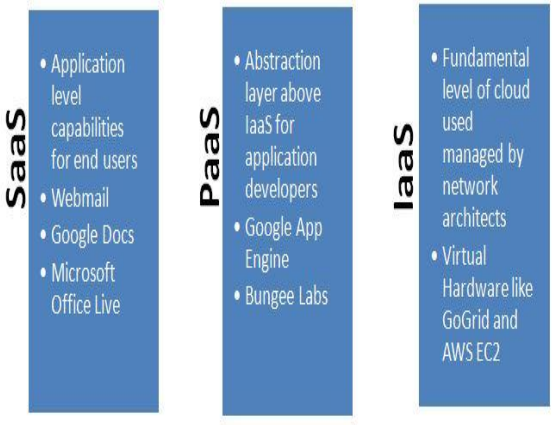

Fig 1: Examples of SaaS, PaaS and Iaas

2. CLOUD, GRID AND DISTRIBUTED COMPUTING

Ian foster et al [3] argue that cloud computing is an evolved form of Grid computing. Cloud computing though similar in many aspects to grid and distributed models is not necessarily the same. Cloud computing is a model where an application doesn't access resources it requires directly, rather it accesses them through a service .It has evolved out of the need for a more economic and scalable form of computing .Distributed computing is the management of numerous computer systems which are limited in memory and processing power. Distributed systems consisting of multiple autonomous computers interact with each other in order to achieve a common goal. A Grid is a hardware and software infrastructure that clusters and integrates high-end computers, networks, databases, and scientific instruments from multiple sources to form a single virtual system. When distributed computing takes place over a network that meets various constraints such as user access and monitoring etc, it is a form of grid computing.

Grids also differ from clouds when it comes to virtualization. Clouds tend to adapt to virtualization for server and application consolidation, dynamic configuration, increased application availability and improved responsiveness. Grids in general have a different user access trust model and their resources are not as abstract as in the cloud model and hence do not depend much on virtualization.

This makes it clear why a cloud would usually require a grid to provide its services, but a grid is not necessarily a cloud or a part of it.

3. SECURITY CONCERNS IN CLOUD COMPUTING

3.1 Insider and Outsider Threats

One of the significant security threats to IT security is the "insider threat" where a trusted insider either unintentionally or maliciously leaks protected information in violation of policy or regulations. These trusted insiders are employees or contractors of the organization and are given access to perform their daily duties and it is difficult to restrict their access. Given its multi-tenant single management nature, matters are more complicated when it comes to cloud computing. The insider threat now expands to a whole new group of people beyond the organizations employees. There is usually no procedure in place ensuring documentation and access logs of computing resources shared by different companies in the cloud.

Outsider threats again is of major concern with any organization as it leaks confidential information outside the organization and holds true for cloud computing as well [4]. Clouds are more associated and networked and often provide more open access to information in the form of API's etc to facilitate user operations. This is taken advantage of by malicious outside users and attackers who exploit the API and breach data. The threats that hackers pose to cloud computing on network level include DNS attacks and sniffer attacks [5]. On the application level the cloud faces threats in the form of Denial of service (DoS) attacks, Distributed Denial of service attacks (DDoS), backdoors, cookie poisoning and also CAPTCHA breaking.

3.2 Loss of data

Data loss refers to the unanticipated loss of data or information. Data loss and leakage can cause financial and reputational loss to the organization .The brand of the organization is tarred and the customer's trust is lost. Data loss can occur in many forms such as downtimes, network or system failures. If a vendor closes down due to legal issues, this might also pose a problem of data loss for the user. Alteration of records of deletion without making prior backups can result in serious data loss issues. Since the amount of data in the cloud is increasing at an exponential rate in the cloud, handling data loss is a major challenge.

3.3 Service Disruption and Account hijacking

Attacks such as phishing, fraud and exploitation of software vulnerabilities help attackers disrupt the cloud service or hijack a user account illegitimately. Service disruptions cause a huge amount of loss for an organisation as far as business and customer base is concerned. [4]. Amazons EC2 and RDS services suffered a major outage for four days in 2011 when their data centre in Northern Virginia was affected. This service disruption affected millions of cloud computing customers [6].

Account hijacking can be a more adverse threat to an organisation. If an attacker gets login credentials to an organisations cloud service, he can manipulate data, monitor transactions, store it for personal use later and hence abrupt the efficient functioning of the organisation. Account hijacking attack methods could be social engineering, phishing mails, and other fraudulent access methods.

3.4 Abuse and unethical use of cloud computing

Cloud providers are usually advertised as a domain of computing with unlimited computing resources, networks and storage and cheap costs coupled with relatively smooth and easy registration process. Some also provide free trial and test periods to their cloud services. Providers with weak registration process give anonymity and are potential targets of abuse. Cloud services are often taken advantage of to create botnet commands and control and host malicious data.

3.5 Confidentiality and Privacy

Privacy concerns exist wherever personal information is collected and stored digitally and improper disclosure control leads to privacy issues.

One of the major factors contributing to the widespread adoption of cloud computing has been its pay-per-use cost model and sharing of resources. To keep a check on insiders and who can have access to what information, a strict policy is inevitable. The cloud must have the ability to prevent attack and give users ability to assess the mechanisms in place [7]. Few points concerning user privacy and confidentiality are:

1. Protecting the user data hosted on the cloud by robust privacy policy.
2. Providing secure technical architecture and applications.
3. Practicing mitigation efforts in case of a breach of security or privacy.

4. MITIGATION CONCEPTS

4.1 Insider and Outsider Threats

In order to alleviate the risk posed by malicious insiders, it is necessary to restrict user access to sensitive data and closely monitor user data. The first step would be to identify any abnormal behaviour that may indicate malicious attacks and automatically block them. All sensitive data usage must be monitored and access to private data must be audited. Systems must be constantly checked and scanned for vulnerabilities and misconfigurations and should be patched immediately. A mapping must be created to identify zones that contain sensitive data and maximum security must be provided. Another important parameter is fair distribution of duties among authorities and eliminating excess rights to be bestowed to an individual.

The risks to cloud computing from hackers can be minimized by following certain countermeasures. A careful monitoring of the network can help identify threats like DoS or DDoS attack whose symptoms include slowing down of network and request from large number of users. Spoofing attacks can be counter by encryption techniques and key exchange based user authorization. SQL-Injections and other interface attacks can be prevented by using techniques such as 'salting' and 'hashing'. CAPTCHA attacks can be prevented by adding more randomness and refraining from use of simple CAPTCHA that are easy to break. Counter measure for cloud malware injection attacks is to check authenticity of received messages by first hashing the requests using a hash function and compare it with hash value of upcoming requests [8].

4.2 Loss of data

The key to data loss prevention is a content and context aware Data Loss Prevention (DLP) system. There is a difference between data loss prevention in general and in the cloud scenario [9]. A third-party is involved in the form of a cloud provider. One needs to provide a system that will enable companies to satisfy diverse security requirements. A DLP works by first identifying sensitive information that needs to be protected and indexes it. It must provide agents to scan for sensitive data and threats. A DLP must be provided at various levels such as the Network layer; storage layer, endpoint DLP and file-level DLP.A DLP must work without any performance degradation of the cloud and must also provide central logging and reporting of all data transfer activities taking place in the cloud.

4.3 Service disruptions and account hijacking

Service disruptions could be prevented by increasing automation and building software and services that survive failures. Increase in capacity of servers handling requests as majorly service disruptions are caused when an unexpected amount of request gets targeted at a particular cluster.

Account hijacking prevention is achieved by disapproving sharing of account credentials, multi-factor authentication techniques and a single-secure sign in feature. Strict monitoring of activities to detect unauthorized activity and unknown sign in to accounts should be in practise to prevent this security concern. Finally a user should be well aware of the terms and conditions, policies and agreements of the service provider providing the cloud service.

4.4 Abuse and nefarious use:

Abuse of cloud computing resources can be mitigated in the following ways [10]:

1. Stricter registration process to check on multiple account creation by single user.
2. Use of CAPTCHAs to make it difficult for automated account creation
3. In Depth introspection of consumer network traffic to monitor and detect suspicious activity.
4. Monitoring public blacklist keys for one's own network block.

4.5 Confidentiality and Privacy

Several measures can be taken to maintain Confidentiality, privacy and integrity in the cloud.

1. Maintaining flexibility of identity management and offering users maximum choice and privacy protection.
2. Ensuring system integrity that indicates whether a system has a trustworthy executing environment [11].
3. Enforcing process integrity by applying software engineering techniques to enhance software security.
4. Techniques like semantic check (applying logic to verification) and trusted path (data is from authenticated user) to check integrity of data.

5. SECURE CLOUD ARCHITECTURE

5.1 Single sign-on and Authentication:

Proper authentication of users or user environments such as a client computer is basic to access control and other IT security functions. It is an essential technology for Cloud-computing environments in which connections to external environments are common and risks are high. To implement strong authentication at user level, organizations should implement a single-sign on for all cloud users to enable users to access multiple application and services thus enabling a strong authentication at user level.

5.2 Isolation of management networks

Cloud infrastructure management networks are how cloud providers access the infrastructure and manage the different components within that infrastructure. Only authorized administrators should have access to this network because control of the management interfaces of the individual virtualization hosts allows for complete control of all of the virtual machines on that host.

5.3 Secure, consistent backups and restoration of cloud-based resources

The service provider should be able to supply the customer with a transparent and secure backup mechanism to allow the customer's cloud-based resources to be backed up on a consistent basis and enable fast restoration in the event of downtime.

5.4 Encryption of critical data

Data encryption adds a layer of protection, even if a system is compromised. Encrypting data in transit is especially important, as that traffic will be traversing a shared network and could potentially be intercepted if an attacker gains access at a critical point in the network. Encrypting the data as it traverses the network makes it much more difficult for an attacker to do anything with intercepted traffic.

5.5 Increased availability:

A cloud consists of critical business data which should always be made available to the users as reducing network downtime will lead to a successful business model and increased revenues for the company. Load balancing at the server end, and dynamic ISP load balancing and backup and restoration of data practises should be employed by the service providers to give the customers an increased availability and satisfaction.

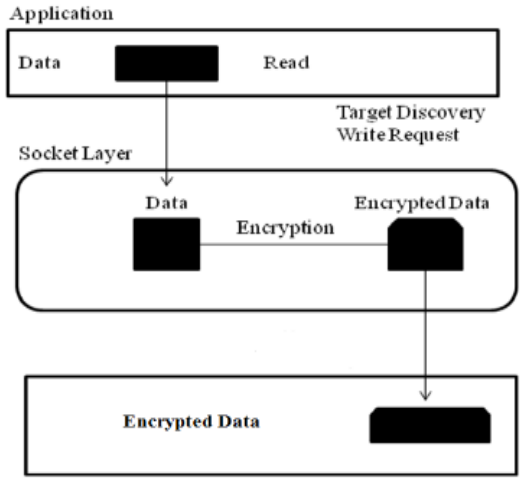

Fig 2: Data Encryption enabling Cloud security

.

5.6 Resource management

The service provider needs to separate and isolate the resources each customer virtual machine uses from other customers' virtual machine resources to prevent DDoS attacks. These attacks are usually caused by log files not having limits or CPU or memory utilization increasing on a single virtual machine through memory leaks or poorly behaving applications.

6. IMPLEMENTATION

This section will describe an implementation of the Single-Sign On (SSO) mechanism discussed above on the Ubuntu Enterprise Cloud. Single sign on is a centralized or unified authorisation process that allows network users to access resources without having to log in separately to each resource. A single action of sign out would terminate access to all the network resources. An SSO can cut down multiple network and applications passwords to a single password which could be used by clients across multiple service providers. The Ubuntu Enterprise Cloud (UEC) is a package stack of applications from Canonical which includes a number of Open Source tools to manage infrastructure powered by Eucalyptus, an open source implementation for the emerging standard of the EC2 API.

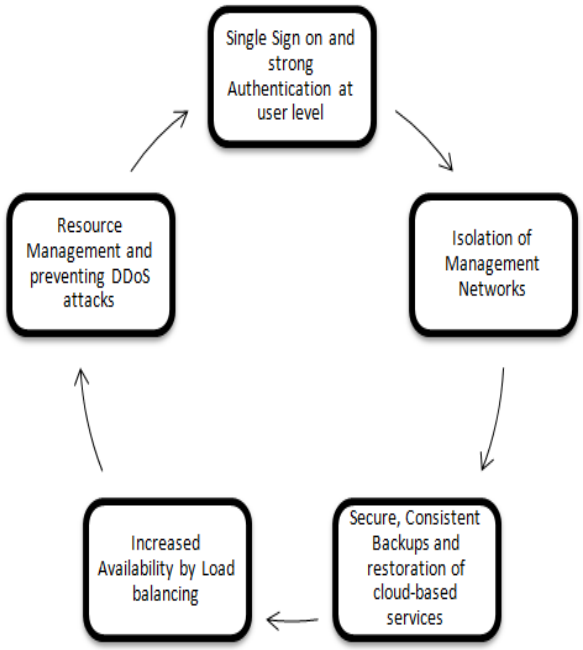

Fig. 3: Secure Cloud Architecture

6.1 Ubuntu Enterprise Cloud Elements

The architecture of Eucalyptus [13], which is the main component of Ubuntu Enterprise Cloud, has been designed as modular set of five simple elements that can be easily scaled:

1. Cloud Controller (CLC)
2. Walrus Storage Controller (WS3)
3. Elastic Block Storage Controller (EBS)
4. Cluster Controller (CC)
5. Node Controller (NC)

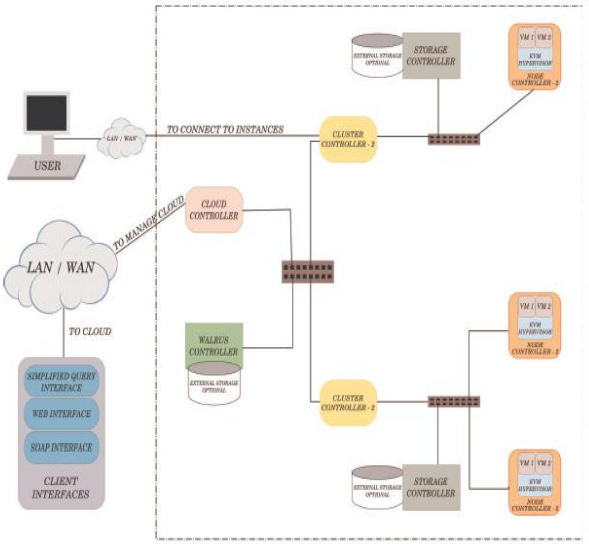

Fig. 4: Ubuntu Enterprise Cloud Components

Table 1: Hardware elements used in implementation

Hardware	Server 1	Server 2	Client
CPU	2.53 GHz Intel Core i5	2.53GHz Intel Core i5	2.53 GHz Intel Core i5
Memory	4 GB	6 GB	4 GB
Disk	7200rpm 500 GB	7200rpm 500 GB	7200rpm 500 GB
Networking	100 Mbps	100 Mbps	100 Mbps
Functionality	CLC, CC and Walrus	NC	Bundling and Web UI Client
No. of NICs	eth0-(Enterprise N/W) eth1-(Eucalyptus N/W)	eth0-(Eucalyptus N/W)	eth0-(Enterprise N/W) eth1-(Eucalyptus N/W)

6.2 Configuration

We implemented Single Sign on using two servers running Ubuntu Server Edition and one client running Ubuntu Desktop Edition. All configuration options were specified based on the topology specified in table 1 given below and nodes were registered on the cluster and availability zone of the cloud was tested based on the parameters specified.

Key pairs were created successfully before running instances of the image. Every instance had 2 addresses associated with it:

a. Private address: Address inside the VM
b. Public address: Address on the CLC and port forwarded (DNAT) to the instance.

When the instance is fully started, the above state changes to a 'running' instance. An IP address is assigned to this instance during the output.

6.3 Setting up a Single Sign on

Single sign on was implemented by using a central authentication server with the authentication server supplying user credentials to the appropriate server, whenever a client requests to use an application on another server. This was developed using PHP and Javascript [14] which enables a client to register on a centralised server and store their credentials. This authentication proxy server uses an LDAP database to maintain client credentials of registered users.

Client authentication was implemented through cURL and SSL, thus creating a robust authentication mechanism over an unsecure network. This ensures reasonable protection from eavesdroppers and man-in-the-middle attacks, provided that adequate cipher suites are used and that the server certificate is verified and trusted. When clients are creating SSO agents with server, information is passed through HTTP requests and uses RSA algorithm to encrypt the data. [14]

6.4 Analysis

In this section we analyse in terms of effectiveness and efficiency, of a specific security initiative to implement a Single Sign-On system. Effectiveness is measured in terms of password compliance, access related incidents, and the time required to provision and de-provision accounts. Efficiency is measured in terms of support workload and effort and a Return on Investment calculation:

The ROI formula [15] used is:

$$\frac{(\text{reduction in effort} + (\text{reduction in incidents} * \text{cost of incident}))}{\text{system cost}}$$

Projected ROI: 97%

Assumptions:

Dollar cost per Account Compromise: $10,000
Loaded Hourly effort cost: $53/hour
Monthly averages used for projection

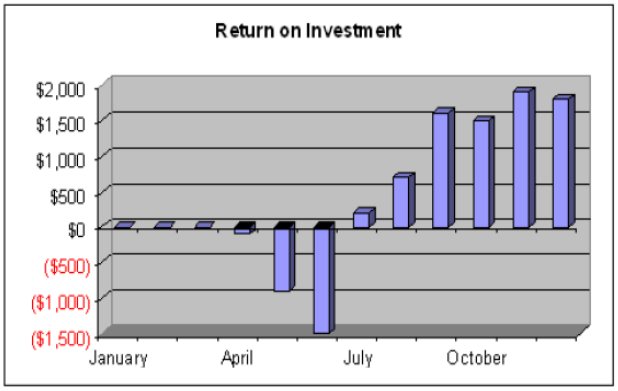

Fig. 5. Return on Investment

7. CONCLUSION

The new era of "cloud computing" offers many benefits, including lower IT costs and greater flexibility for businesses as well as new and easier ways for individuals to connect, share common interests, and access information. The fundamental principles, practices, and tools that have evolved over the past two decades to help protect users on the Internet remain effective in the cloud computing realm. This paper presented a complete structure of cloud computing, major security risks and their mitigation and implementation of a secure cloud architecture using which service provides could offer extensive services to customers with complete security. Single sign-on greatly enhances the usability

of the Cloud environment by allowing users to authenticate once to access applications on multiple machines. It is essential to know the fact that a single measure cannot completely resolve the security issue, however, with a correct security strategy, multiple layers of security control it is possible to reduce the threat and make the cloud computing era a successful revolution.

7. REFERENCES

[1] Farhan Bashir, Shaikh, "Security threats in Cloud Computing" *6th International conference on Internet Technology and Secure Transactions*, IEEE 2011

[2] Jianfeng Yang, Zhibin Chen, "Cloud Computing Security issues" 978-1-4244-5392-4/10 2010 IEEE

[3] Ian Foster, Yong Zhao, Ioan Raicu, Shiyong Lu. "Cloud Computing and Grid Computing 360-Degree Compared", IEEE Grid Computing Environments (GCE08) 2008, co-located with IEEE/ACM Supercomputing 2008.

[4] Alok Tripathy, Abhinav Mishra "Cloud computing security considerations" IEEE, 2011

[5] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, Sugata Sanyal: A Survey on Security Issues in Cloud Computing CoRR abs/1109.5388: (2011)

[6]Amazon Web services: Official Amazon report: http://aws.amazon.com

[7] Rocha F. "The Final Frontier: Confidentiality and Privacy in the Cloud" IEEE Volume:44 Issue:9 Sept. 2011

[8] Sara Qaisar ,Kausar Fiaz Khawaja "Cloud Computing: Network/Security Threats and Countermeasures" *Interdisciplinary Journal of Contempory research in business* January 2012 Vol.3, No. 9

[9] T. Takebayashi et al.: Data Loss Prevention Technologies FUJITSU Sci. Tech. J., Vol. 46, No. 1 (January 2010)

[10] David Q. Liu Shilpashree Srinivasamurthy "Survey on Cloud Computing Security" IEEE-2011

[11] Jeff Naruchitparames and Mehmet Hadi Gunes, "Enhancing Data Privacy and Integrity in the Cloud".

[12] W. Mao, F. Yan, and C. Chen, "Daonity: grid security with behaviour conformity from trusted computing," in *1st ACM workshop on Scalable trusted computing*. ACM, 2006, pp. 43–46.

[13] Johnson D, Kiran Murari, Murthy Raju, Suseendran RB, Yogesh Girikumar, "Eucalyptus Beginner's Guide - UEC Edition", v1.0, 25 May 2010, CSS Corp. Pvt. Ltd.

[14] http://techportal.ibuildings.com/2009/03/31/php-and-the-cloud/

[15] Andrew Sudbury, Director, Security Metrics Design & Best Practices, "Highlights of a Security Scorecard Project", ClearPoint Metrics.