Research Article Impact Factor: 0.621 ISSN: 2319-507X
Salim Amdani, IJPRET, 2014; Volume 2 (8): 17-26 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

EVOLUTION OF CLOUD SECURITY SINGLE TO MULTI CLOUD SYSTEMS

DR. SALIM Y. AMDANI[1], GEETA N.JAMODE[2]

1. Prof., Department of Computer Science and Engineering, Babasaheb Naik College of Engineering, Pusad, Maharashtra, India.
2. M.E Student, Department of Computer Science and Engineering, Babasaheb Naik College of Engineering, Pusad, Maharashtra, India.

Accepted Date: 15/02/2014 ; Published Date: 01/04/2014

Abstract: Cloud computing security is the sub domain of network security broadly, information security. It consist broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be untrusted. Dealing with "single cloud" providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. A movement towards "multi-clouds", or in other words, "interclouds" or "cloud-of-clouds" has emerged recently. This paper reviews recent research related to single and multi-cloud security and addresses possible solutions. It is found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. This work aims to promote the use of multicourse due to its ability to reduce security risks that affect the cloud computing user.

Keywords: Cloud computing, single cloud, multi-clouds, cloud storage, data integrity, data intrusion, service availability

Corresponding Author: DR. SALIM Y. AMDANI

Access Online On:

www.ijpret.com

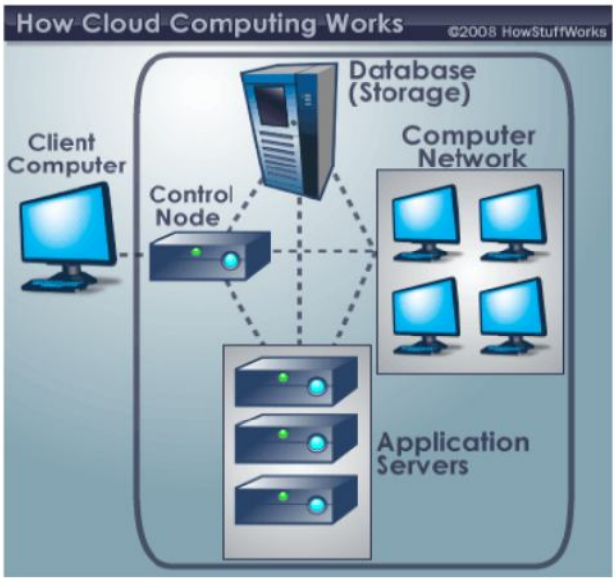
How to Cite This Article:

Salim Amdani, IJPRET, 2014; Volume 2 (8): 17-26

PAPER-QR CODE

INTRODUCTION

Cloud computing is a term used to describe both a platform and type of application. As a platform it supplies, configures, reconfigures the servers while the servers can be physical machines or virtual machines. On the other hand cloud computing describes applications that are extended to be accessible through the internet and for this purpose large data centers and powerful servers are used to host the web applications and web services.



A. *Benefits of Cloud Computing*

The benefits of cloud computing are Reduced Data Leakage, Decrease evidence acquisition time, they eliminate or reduce service downtime, they Forensic readiness, they decrease evidence.

B. *Drawbacks of Cloud Computing*

Few of the disadvantages associated with Cloud computing are:

- High Speed Internet Required
- Constant Internet Connection

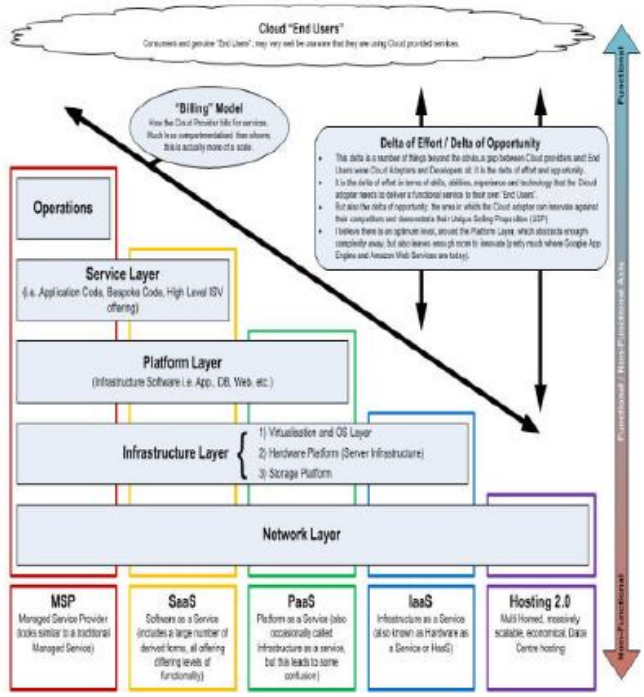
Limited Features

Data Stored is not secure

I. METHODOLOGY

Cloud architecture, the systems architecture of the software systems involved in the delivery of cloud computing, comprises hardware and software designed by a cloud architect who typically works for a cloud integrator. It typically involves multiple cloud components communicating with each other over application programming interfaces, usually web services.

Cloud architecture extends to the client, where web browsers and/or software applications access cloud applications.



Cloud storage architecture is loosely coupled, where metadata operations are centralized enabling the data nodes to scale into the hundreds, each independently delivering data to applications or user.

II. A TYPICAL CLOUD COMPUTING SYSTEM:

Soon, there may be an alternative for executives like you. Instead of installing a suite of software for each computer, you'd only have to load one application. That application would allow workers to log into a Web-based service which hosts all the programs the user would

need for his or her job. Remote machines owned by another company would run everything from e-mail to word processing to complex data analysis programs. It's called cloud computing, and it could change the entire computer industry. In a cloud computing system, there's a significant workload shift. Local computers no longer have to do all the heavy lifting when it comes to running applications. The network of computers that make up the cloud handles them instead. Hardware and software demands on the user's side decrease. The only thing the user's computer needs to be able to run is the cloud computing systems interface software, which can be as simple as a Web browser, and the cloud's network takes care of the rest.

There's a good chance you've already used some form of cloud computing. If we have an e-mail account with a Web-based e-mail service like Hotmail, Yahoo! Mail or Gmail, then we've had some experience with cloud computing. Instead of running an e-mail program on our computer, we log in to a Web e-mail account remotely. The software and storage for our account doesn't exist on our computer – it's on the service's computer cloud.

III. WHAT IS DRIVING CLOUD COMPUTING?

The cloud computing is driving in two types of categories

i. Customer Perspective

-In one word: economics

-Faster, simpler, cheaper to use cloud computation.

-No upfront capital required for servers and storage.

-No ongoing for operational expenses for running data centre.

-Application can be run from anywhere.

ii. Vendor Perspective

Easier for application vendors to reach new customers.

-Lowest cost way of delivering and supporting applications.

-Ability to use commodity server and storage hardware.

-Ability to drive down data center operational costs.

-Computer hardware (Dell, HP, IBM,Sun Microsystems)

-Storage (Sun Microsystems, EMC,IBM)

-Infrastructure (Cisco Systems)

-Computer software (3tera, Hadoop IBM, RightScale)

-Operating systems (Solaris, AIX, Linux including Red Hat)

Platform virtualization (Citrix,Microsoft, VMware, Sun xVM, IBM)

V. SECRET SHARING ALGORITHMS

Data stored in the cloud can be compromised or lost. So, we have to come up with a way to secure those files. We can encrypt them before storing them in the cloud, which sorts out the disclosure aspects. However, what if the data is lost due to some catastrophe befalling the cloud service provider? We could store it on more than one cloud service and encrypt it before we send it off[10]. Each of them will have the same file. What if we use an insecure, easily guessable password to protect the 2012 45th Hawaii International Conference on System? Sciences file, or the same one to protect all files? I have often thought that secret sharing algorithms could be employed to good effect in these circumstances instead.

VI. EXISTING SYSTEM

a) Disadvantages

1. Cloud providers should address privacy and security issues as a matter of high and urgent priority.

2. Dealing with “single cloud” providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud.

VII. SECURITY RISKS IN CLOUD COMPUTING

There are three important security risks identified in cloud computing:

1. Data Integrity

2. Data Intrusion

3. Service Availability

1. Data Integrity

One of the most important issues related to cloud security risks is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider[3]. Cachinet al. gives examples of the risk of attacks from both inside and outside the cloud one provider, such as the recently attacked Red Hat Linux's distribution servers. Of the solutions that they propose is to use a Byzantine fault-tolerant replication protocol within the cloud[9]. Hendricks Et Al. State that this solution can avoid data corruption caused by some components in the cloud. However, Cachinet al. Claim that using the Byzantine fault tolerant replication protocol within the cloud is unsuitable due to the fact that the servers belonging to cloud providers use the same system installations and are physically located in the same place. [1]

2. Data Intrusion

According to Garfinkel, another security risk that may occur with a cloud provider, such as the Amazon cloud service, is a

hacked password or data intrusion. If someone gains access to an Amazon account password, they will be able to access all of the account's instances and resources. Thus the stolen password allows the hacker to erase all the information inside any virtual machine instance for the stolen user account, modify it, or even disable its services [1]. Furthermore, there is a possibility for the user's email(Amazon user name) to be hacked (see for a discussion of the potential risks of email), and since Amazon allows a lost password to be reset by email, the hacker may still be able to log in to the account after receiving the new reset password.

3. Service Availability

Another major concern in cloud services is service availability. Amazon [6] mentions in its licensing agreement that it is possible that the service might be unavailable from time to time. The user's web service may terminate for any reason at any time if any user's files break the cloud storage policy. In addition, if any damage occurs to any Amazon web service and the service fail, in this case there will be no charge to the Amazon Company for this failure. Companies seeking to protect services from such failure need measures such as backups or use of multiple providers [1].

- PROPOSED SYSTEM:

This paper focuses on the issues related to the data security aspect of cloud computing. As data and information will be shared with a third party, cloud computing users want to avoid an untrusted cloud provider. Protecting private and important information, such as credit card details or a patient's medical records from attackers or malicious insiders is of critical importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing is reviewed [2].

The cloud computing doesn't end with single cloud. In recent years, there has been a move towards "multi clouds", "inter cloud" or "cloud-of-clouds".

Multi-cloud technique is the use of two or more cloud services to minimize the risk of large amount of data loss or temporary fault in the computers due to a localized component failure in a cloud computing environment.

Such a failure may occur in hardware, software, or infrastructure. A multi-cloud approach is also used to control the traffic from different customer bases or partners through the fastest possible parts of the network.

1. Dep Sky System: Multi-Cloud Model

Bessani et al. [8] present a virtual storage cloud system called DepSky which consists of a combination of different clouds to build a cloud-of-clouds. The DepSky system addresses the availability and the confidentiality of data in their storage system by using multi-cloud providers, the following figure illustrates the architecture of DepSky.

DEPSKY is accessed by its users by invoking operations in several individual clouds. It addresses four important limitations of cloud computing for data storage in the following way:-

1. Loss of availability

2. Loss and Correction of data

3. Loss of privacy

4. Vendor lock-In

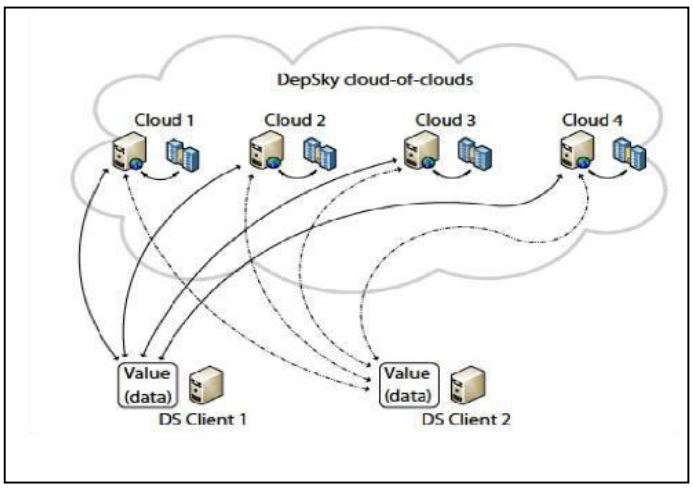


Fig: DepSky Architecture

The data outsourced by clients can store in any cloud. It does mean that the multiple clouds work together. This will automatically improve **service availability** and **reduce the risk of losing data** as well. With regard to internal theft strict measures are to be used by cloud service providers.

The DepSky system model contains three parts: readers, writers, and four cloud storage providers, where readers and writers are the client's tasks. Bessani et al.explain the difference between readers and writers for cloud storage. Readers can fail arbitrarily (for example, they can fail by crashing, they can fail from time to time and then display any behaviour) whereas, writers only fail by crashing. [5][8]

2. Analysis of Multi-Clouds

The main purpose to move from single to multi cloud is by distributing reliability, trust, and security among multiple cloud providers.

Actually RAID is used in disks for data storage, based on this RACS (Redundant Array of Cloud Storage) is developed for multiple cloud storage. Abu-Libdeh et al. [3] assume that to avoid "vender lock-in", distributing a user‟s data among multiple clouds is a helpful solution. Mohammad et al. This replication also decreases the cost of switching providers and offers better fault tolerance. Therefore, the storage load will be spread among several providers as a result of the RACS proxy.

Another example to control multiple clouds is HAIL (High Availability and Integrity Layer). HAIL is a distributed cryptographic system that allows a set of servers to secure the client's stored data is retrievable and integral. HAIL provides a software layer to address availability and integrity of the stored data in an intercloud [10].

IX. CONCLUSION

Cloud computing is a powerful new abstraction for large scale data processing systems which is scalable, reliable and available. Cloud computing security is still considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. Furthermore, data intrusion leads to many problems for the users of cloud computing. In cloud computing, there are large self-managed server pools available which reduces the overhead and eliminates management headache. Cloud computing services can also grow and shrink according to need. Cloud computing is particularly valuable to small and medium businesses, where effective and affordable IT tools are critical to helping them become more productive without spending lots of money on in-house resources and technical equipment. Also it is a new emerging architecture needed to expand the Internet to become the computing platform of the future. The purpose of this work is to review the recent research on single clouds and multi-clouds to address the security risks and solutions. We have found that much research has been done to ensure the security of the single cloud and cloud storage whereas multiclouds have received less attention in the area of security. We support the migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

REFERENCES

1. Cloud Computing Security: *From Single to Multi-Clouds* Mohammed A.AlZain #, Eric Pardede #, Ben Soh #, James A. Thom* 2012 45th Hawaii International Conference on System\ Sciences, 2012 IEEE.
2. Abraham, G. Chockler, I. Keidar and D. Malkhi, "Byzantine disk paxos: optimal resilience with Byzantine shared memory", Distributed Computing, 18(5), 2006, pp. 387-408.
3. H. Abu-Libdeh, L. Princehouse and H.Weatherspoon, "RACS: a case for Cloud storage diversity", SoCC'10:Proc. 1st ACM *symposium on Cloud Computing,* 2010, pp. 229-240.
C. Agrawal, A. El Abbadi, F. Emekci and A.Metwally, *"Database Management as a Service:* Challenges and Opportunities", ICDE'09:Proc.25thIntl. Conf. on Data Engineering, 2009, pp. 1709-1716.

4. M.A. AlZain and E. Pardede, "*Using Multi Shares for Ensuring Privacy in Database-as-a-Service",* 44th Hawaii Intl. Conf. on System Sciences (HICSS), 2011, pp. 1-9.
5. Amazon,Amazon Web Services,Web Service licensing agreement,October3,2006.
6. G. Ateniese, R. Burns, R. Curtmola, J.Herring, L. Kissner, Z. Peterson and D Song, "Provable data possession at untrusted stores", Proc. 14th ACM Conf. on Computer and communications security, 2007, pp. 598-609.
A. Bessani, M. Correia B. Quaresma,F. Andre and P. Sousa "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc6thConf. On Computer systems, 2011, pp. 31-4
7. K. Birman, G. Chockler and R. van Renesse,"T*oward a cloud computing researchagenda*", SIGACT News, 40, 2009, pp. 68-80.
8. K.D. Bowers, A. Juels and A. Oprea, "HAIL: *A high-availability and integrity layer for cloud storage",* CCS'09: Proc. 16th ACM Conf. on Computer and communications security, 2009, pp.187-198.