Analyzing Horizontal Integration among Soa, Cloud Computing and Grid Computing

GJCST Computing Classification
C 1.4, C 2.1

Mr. Krunal D. Trivedi[1], Mr. Kamaljit I. Lakhtaria[2], Mrs. Palak R. Shah[3],Dr.N.J.Patel[4]

***Abstract*- Cloud computing is among emerging technologies for high speed, complex computing. Cloud computing means anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Virtual resources and computing assets are accessed through the cloud, including not only externally hosted services but also those provided globally by companies. This provides the basis for the next generation of enterprise data centre which, like the Internet, will provide extreme scalability and fast access to networked users.**

In this article, we analyze different standards for Messaging, Security, standards for Application Development and the role of Open Virtualization Format (OVF) in virtualized environment for Cloud Computing. We have suggested security aspect with a proposed architecture for relationship and intersection between Service Oriented Architecture, Grid Computing and Cloud Computing.

Keywords- SOA, Cloud computing, IaaS, PaaS, SaaS.

I. INTRODUCTION

A. To Cloud Computing And Architecture

A cloud service has three discrete characteristics that discriminate it from traditional hosting. It is sold on demand, typically by the minute or the hour; it is elastic -- a user can have as much or as little of a service as they want at any given time; and the service is fully managed by the provider like payment and any search services.

The diagram illustrates (Figure 1) the component architecture. Virtualized Infrastructure allows business services to move directly across virtualized infrastructure resources in a very efficient manner.

About- [1,2]MCA Department, Acharya Motibhai Patel Institute of Computer Studies, Ganpat University, Mehsana Gujarat, INDIA, Email: trivedi.kunal@gmail.com, Email: palak.kunal@gmail.com

About-[3]MCA Department, Atmiya Institute of Technology & Science, Rajkot, Gujarat, INDIA

Email: kamaljit.ilakhtaria@gmail.com

About[4]-professor and head U V patel college of engineering E-mail narendraj.patel@ganpatuniversity.ac.in

Security standards, Protocols are defined in Security Management. This Layer also defined the various processes, procedures, and practices necessary for implementing a security program.

Virtualized applications are decouple from the underlying hardware, operating system, storage, and network to enable flexibility in deployment. Virtualized Application servers that can decorate of grid execution coupled with Service Oriented Architectures. And this intersection of Cloud, SOA and Grid provide the greatest scalability to meet the business requirements.

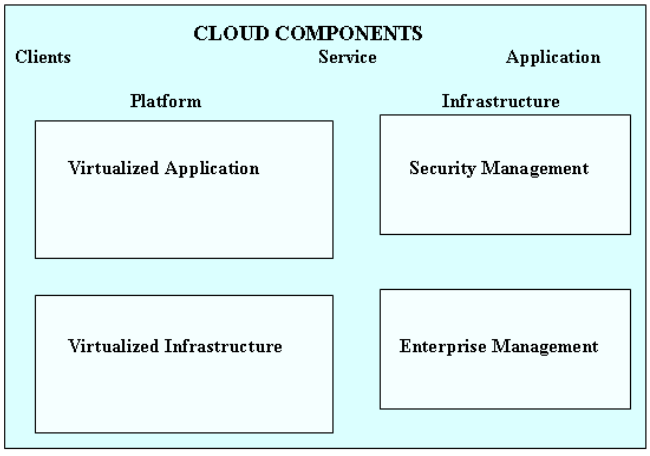

Figure 1: Cloud Components Architecture

Enterprise management provides top-down, end-to-end management of the virtualized infrastructure and applications for business solutions. This layer also handles the full lifecycle of virtualized resources and provides additional common infrastructure elements for service level management, policy management, license management, and disaster recovery. Here is the detail explanation of each Cloud Components.

Table 1: Examples of individual Cloud Components

Cloud Components	Examples
Clients	Mobile like iPhone, Windows Mobile. Thin client like CherryPal, Zonbu. Thick client like Microsoft Internet Explorer, Mozilla Firefox, Google Chrome etc.
Services	Identity (Open Authentication, Open ID) Payments (Amazon Flexible Payments Service, Google Checkout) Mapping (Google Maps, Yahoo! Maps, MapQuest) Search (Alexa, Google Custom Search, Yahoo! BOSS) Video Games (OnLive) Live chat (LivePerson)
Application	Peer-to-peer / volunteer computing (Bittorrent, Skype) Web application (Twitter)
Platform	Amazon.com, eBay, Google, iTunes, and YouTube.
Infrastructure	Full virtualization (GoGrid, Skytap, iland) Compute (Amazon EC2, Rackspace Cloud Servers, Savvis) Platform (Force.com)

B. *Example Of Cloud Computing Www.Facebook.Com*

Face Book statistics are mentioned here

i. Facebook may have 175 million active users, 11m of which are Canadians. (As on January 2010)

ii. Facebook is the world's largest photo site, at over 850 million images uploaded per month.

iii. Facebook uses partitioned/denormalized MySQL databases, but uses extensive caching (using —mem-cache-D") to minimize the number of database requests:

- 10,000 PHP webservers, 1,000 memcached servers, with 15TB RAM
- approximately 2000 MySQL servers with 25 terabytes of RAM
- 10 million requests/sec from the web, reduced to 500K/sec to MySQL through the use of memcached.

iv. The Facebook front-end tier dumps logs and database extractions into Hadoop/Hive. Hive is Facebook's data warehouse technology that is built over Hadoop: it support an SQL-like query language with support for joins, grouping, and aggregation. From Hive, data summaries are exported into Business Intellignece applications and/or into an Oracle RAC for analysis, including usage trends, ad-hoc queries, ad optimization, and spam detection. For Facebook, their Hive data warehouse stores 10TB of new data per day (2TB compressed) and totals 500TB compressed, over 600+ nodes with 50+ engineers supporting the warehouse.

II. CLOUD COMPUTING STANDARDS

Cloud Computing have many preferable standards for Messaging, Security and for Application developer.

Cloud computing growth facilitated with powerful and light weight open source standards

A. *Open Virtualization Format*

The Open Virtualization Format Specification was prepared by the System Virtualization, Partitioning, and Clustering Working Group of the DMTF. OVF 1.0 is the First industry standard to enable interoperability within virtualized environments.

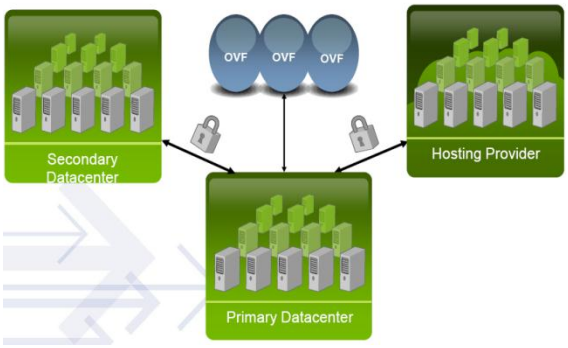

Figure 2: How Open Virtualized Format deals with provider to Data Centre

The Open Virtualization Format (OVF) Specification describes an open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines. The key properties of the format are as follows:

i. Optimized for distribution: OVF supports content verification and integrity checking based on industry-standard public key infrastructure.

ii. Supports both single VM and multiple-VM configurations: OVF supports both standard single VM packages and packages containing complex, multi-tier services consisting of multiple interdependent VMs.

iii. Vendor and platform independent: OVF does not rely on the use of a specific host platform, virtualization platform, or guest operating system.
iv. Extensible: OVF is immediately useful — and extensible. It is designed to be extended as the industry moves forward with virtual appliance technology. It also supports and permits the encoding of vendor-specific metadata to support specific vertical markets.
v. Localizable: OVF supports user-visible descriptions in multiple locales, and it supports localization of the interactive processes during installation of an appliance. This capability allows a single packaged appliance to serve multiple market opportunities.
vi. Open standard: OVF has arisen from the collaboration of key vendors in the industry, and it is developed in an accepted industry forum as a future standard for portable virtual machines.
vii. Security: The OVF specifies procedures and technologies to permit integrity checking of the virtual machines (VM) to ensure that they have not been modified since the package was produced. This enhances security of the format and will help to alleviate security concerns of users who adopt virtual appliances produced by third parties.

B. LAMP, JSON, AJAX For Application Developer

LAMP- Linux, Apache, Postgre SQL, and PHP (or Perl or Python) is open source web platform that can be used to run dynamic web sites and servers. JSON- Java Script Object Notation is a lightweight computer data interchange format and Asynchronous Java Script Xml are the application standards that can provide that are commonly used across the Internet in browsers, for transferring data, sending messages, and securing data.

C. Web Services, Atom And Atom Publishing Protocol For Messaging

i. Web Services: For consistent and loosely-coupled architectures. Cloud are constructed with web services as the system interface such as Amazon Web Services, Google Apps, and Salesforce.com CRM.
ii. Atom: The Atom Syndication Format is an XML language used for web feeds. And it allows software programs to check for updates on a website published. To provide a web feed, a site owner may use specialized software such as a content management system that publishes a list or "feed" of recent articles or content in a standardized and machine-readable format. Web feeds are used by the blog community to share recent entries' headlines, full text, and even attached multimedia files. Atom also provides a standard way to export an entire blog, or parts of it, for backup or for importing into other blog systems.
iii. Atom Publishing Protocol: The Atom Publishing Protocol (AtomPub or APP) is a simple HTTP-based protocol for creating and updating web resources. APP mechanisms required for the exchange of rich and meaningful content via a process known as Representational State Transfer in cloud application. Atom publishing protocol operates on collections of Web resources.

D. Open Authentication And Open ID For Security

Security standards define the processes, procedures, and practices necessary for implementing a security program. These standards have several processes and procedure those are applying to cloud related IT activities and ensure a secure environment. And the environment is maintained by privacy and security of confidential information. Security standards are based on a set of key principles intended to protect this type of trusted environment. Messaging standards, especially for security in the cloud, must also include nearly all the same considerations as any other IT security endeavours. The following protocols are used in the cloud environment.

i. Open Authentication: Open Authentication is an open protocol, initiated to allow secure API authorization in a simple, standardized method for various types of web applications. Open Authentication provides users access to their data while protecting account credentials. Open Authentication also allows users to grant access to their information, which is shared by the service provider and consumers without sharing all of their identity.
ii. Open ID: Open ID is an open, decentralized standard for user authentication and access control that allows users to log onto many services using the same digital identity. It is a single-sign-on (SSO) method of access control. As such, it replaces the common log-in process (i.e., a log-in name and a password) by allowing users to log in once and gain access to resources across participating systems.

III. INTERSECTION BETWEEN CLOUD, SERVICE ORIENTED ARCHITECTURE AND GRID COMPUTING

Cloud Computing expands SOA by adding scalability and Grid Computing. Cloud computing is a means of computing 'services' that are provided over the internet and can scale dynamically and is based on virtualized resources. Cloud Service Providers includes IBM , Amazon , Google , Microsoft , Yahoo etc. These applications may need many computers. And here the computing resources are shared by multiple clients/consumers. Internally, they run a grid, but it is hidden from you.

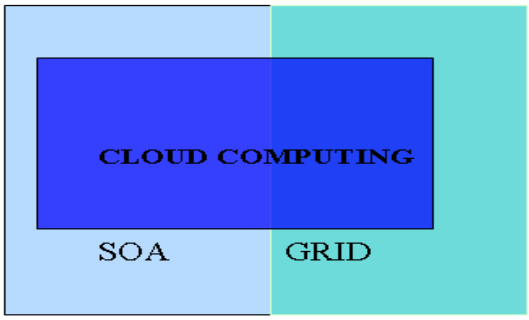

Figure 3: Intersection between SOA, Cloud and Grid.

SOA provides the evolutionary step to cloud computing by creating the necessary interfaces from the IT infrastructure to the cloud outside the enterprise. Cloud computing essentially becomes an extension of SOA.

SOA is derived from architecture and a methodology. Since cloud computing is typically driven from the view of business resources that are needed,

Another evolutionary step that cloud computing has taken from the SOA model is to architect and design services into the cloud so that it can expand and be accessed as needed. Expanding services in an SOA is typically a difficult and expensive process.

However, cloud computing is accelerating the adoption of SOA by providing aspects of SOA on-demand. SOA can learn a lot from the clouds, and the clouds can learn a lot from SOA."

Differentiating between SOA and cloud computing can be confusing because they overlap in some areas but are fundamentally different. SOA delivers web services from applications to other programs, whereas the cloud is about delivering software services to end users and running code. Thus the cloud-versus-SOA debate is like comparing apples and oranges. The true success of SOA application depends widely on its deployment in the cloud and taking advantage of its elasticity.

IV. Challenges and Security Issues for Cloud Environment

i. Cloud applications undergo constant feature additions, and users must keep up to date with application improvements to be sure they are protected. The speed at which applications will change in the cloud will affect both the SDLC and security.

ii. Data integrity means ensuring that data is identically maintained during any operation (such as transfer, storage, or retrieval). Put simply, data integrity is assurance that the data is consistent and correct. Ensuring the integrity of the data really means that it changes only in response to authorized transactions. This sounds good, but you must remember that a common standard to ensure data integrity does not yet exist.

iii. Any information stored locally on a computer can be stored in a cloud, including email, word processing documents, spreadsheets, videos, health records, photographs, tax or other financial information, business plans, PowerPoint presentations, accounting information, advertising campaigns, sales numbers, appointment calendars, address books, and more. The entire contents of a user‘s storage device may be stored with a single cloud provider or with many cloud providers. Whenever an individual, a business, a government agency, or other entity shares information in the cloud, privacy or confidentiality questions may arise.

iv. Even if data is securely stored in a cloud, many factors can temporarily disrupt access to the data, such as network outages, denial of service attacks against the service provider, and a major failure of the service provider infrastructure. It may be a challenge to host and maintain intranet and access restricted sites (government, defense, institutional.)

v. If information is encrypted while passing through the cloud, who controls the encryption/decryption keys? Is it the customer or the cloud vendor?

vi. If your data is not available or is completely wiped out due to a disaster, can they replicate that data for you? How soon? How much of it?

vii. The virtual machines must be self-defending, effectively moving the perimeter to the virtual machine itself. Enterprise perimeter security (i.e., firewalls, demilitarized zones, network segmentation, intrusion detection and prevention systems [IDS/IPS], monitoring tools, and the associated security policies) only controls the data that resides and transits behind the perimeter.

V. Conclusion

Expanding services in an SOA is typically a difficult and expensive process. So Cloud architecture attached to grid computing ensures that the SOA applications take advantage of the elasticity of cloud computing environment and grid computing able to process a service within a finite amount of time. Cloud computing has been criticized for limiting the freedom of users and making them dependent on the cloud computing provider, and some critics have alleged that it is only possible to use applications/services that the provider willing to offer. Virtualization related issues will be satisfactorily resolved and network intrusion detection and prevention system for cloud is appearing as this new technology matures.

VI. REFERENCES

1) Andy Bechtolsheim Chairman & Co-founder, Arista Networks- Cloud Computing, November 12th, 2008.
2) Daniel J. Abadi, Data Management in the Cloud: Limitations and Opportunities.
3) David Linthicum, SOA cloud computing relationship leaves some folks in a fog, Mar 09, 2009.
4) Ejaz Jamil, What really is SOA. A comparison with Cloud Computing, Web 2.0, SaaS, WOA, Web Services, PaaS and others.
5) Fred cummins, SOA and Cloud: Business Necessity for Small to Medium Sized Businesses, September 2009.
6) Joe McKendrick,Connecting the Dots Between SOA and Cloud,June 29, 2009.
7) John W. Rittinghouse, James F. Ransome:Cloud Computing Implementation, Management and Security.
8) Marcia Savage, Security challenges with cloud computing services, Information Security magazine21 Sep 2009 | SearchSecurity.com .
9) Nikita Ivanov, 20 Real-Life Challenges of Cloud Computing.
10) Oracle White Paper in Enterprise Architecture – Architectural Strategies for Cloud Computing.
11) Paul Krill, The cloud-SOA connection, February 2009.
12) SOA Consortium, Finding the Intersections of SOA and Cloud Computing.
13) Sun Cloud Computing.
14) The Aspen Institute, Identity in the Age of Cloud Computing: The next-generation Internet‘s impact on business, governance and social interaction, 2009.
15) http://www.dmtf.org/standards/published documents/DSP0243_1.1.0.pdf