Approach for Application on Cloud Computing

[1]Shiv Kumar, [2]Bimlendu Verma , [3]Archana Neog

**[1] Faculty of Engineering and Technology, Mewar University,
NH-9 Gangrar, Rajasthan-312901, India**

**[2] Faculty of Engineering and Technology, Mewar University,
NH-9 Gangrar, Rajasthan-312901, India**

**[3] C.V.R.C.E. Bhubaneswar, Biju Patnaik University of Technology
Rourkela, Odisa, India**

Abstract

A web application is any application using web browser as client or we can say that it is a dynamic version of a web or application server. There are two types of web applications based on orientation:

1. A presentation-oriented web application generates interactive web pages containing various types of markup language like HTML, XML etc. and dynamic content in response to requests.
2. A service-oriented web application implements the endpoint of a web service.

Web applications commonly use server-side script like ASP, PHP, etc and client-side script like HTML, JavaScript, etc. to develop the application. Web applications are used in the field of banking sector, insurance sector, marketing, finance, services etc.

"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 be rapidly provisioned and released with minimal management effort or service provider interaction." - U.S. National Institute of Standards and Technology (NIST)

A general and simple cloud computing definition is using web applications and/or server services that you pay to access rather than software or hardware that you buy and install.

.

Keywords: *Browser, Cloud computing, Web application, SAAS, Protocols, Standard, Legal*

1. Introduction

Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth.

A simple example of cloud computing is Yahoo email, Gmail, or Hotmail etc. You dont need a software or a server to use them. All consumer would need just an internet connection and you can start sending emails. The server and email management software is all on the cloud (internet) and is totally managed by the cloud service provider Yahoo, Google etc

Cloud computing is considered a priority by executive teams in 69% of the organizations as surveyed. Among large companies, the percentage is slightly higher (71%) than for medium (67%) and small companies (68%).[1]

However, it's actually small companies that are leading the way in terms of cloud usage. Overall, 76% of respondents said their companies were using cloud services or planned to do so within the next 24 months — with 78% of small companies already using or planning to use cloud, compared with 73% of both large and medium-size companies[1]

From a user's point of view, a good cloud computing definition is using web applications and/or server services that you pay to access rather than software or hardware that you buy and install.

2. Web application and Cloud Computing

Generally web components provide the dynamic extension capabilities for a web server. Web components are Java servlets, JSP pages, or web service endpoints in java platform. The interaction between a web client and a web application is done using HTTP Request and HTTP Response. The client sends an HTTP request to the web server. A web server that implements Java Servlet and Java Server Pages technology converts the request into an HTTPServletRequest object. This object is delivered to a web component, which can interact with JavaBeans components or a database to generate dynamic content. The web component can then generate an HTTPServletResponse or it can pass the request to another web component. Eventually a web component generates an HTTPServletResponse object. The web server converts this object to an HTTP response and returns it to the client.

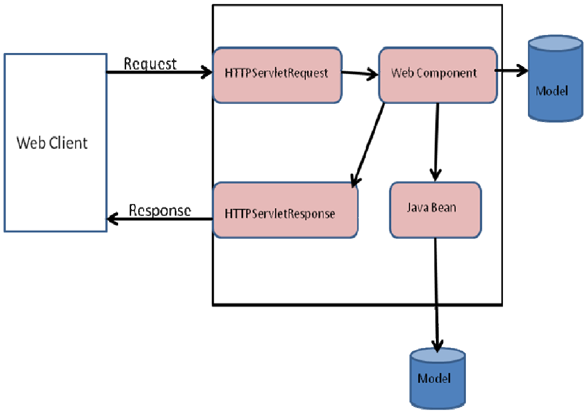

Fig. 1 Proposed beam former.

As we know that cloud computing is using web applications and/or server services that you pay to access rather than software or hardware that you buy and install. There are three types of cloud service models: Infrastructure, Platform and Software as a Service. The software layer builds upon platform, while platform builds upon infrastructure.[2]

2.1 Infrastructure as a Service (IaaS)

With this model, a customer rents physical facilities, connectivity, and hardware to deploy customer software, operating systems and applications; specific IaaS vendors include “Amazon EC2, Go Grid, and FlexiScale.”[3] With IaaS, a customer is not required to manage/purchase servers and network infrastructure equipment, even though configuration management is still required. One disadvantage to IaaS is that bandwidth delays may occur with remote execution.[4]

Infrastructures as a Service cloud computing companies are:

A. Amazon's offerings include S3 (Data storage/file system), Simple DB (non- relational database) and EC2 (computing servers).

B. Rack space’s offerings include Cloud Drive (Data storage/file system), Cloud Sites (web site hosting on cloud) and Cloud Servers (computing servers).

C. Go Grid’s offerings include Cloud Hosting (web site hosting on cloud) and Cloud Storage (Data storage/file system).

D. IBM's offerings include Smart Business Storage Cloud and Computing on Demand (CoD).

E. AT&T's offerings include Synaptic Storage as a service and Synaptic Compute as a service.

2.2 Platform as a Service (PaaS)

This model enables a customer to rent a platform (hardware, storage, or virtual computers) to deploy its own specifically created applications; applications are then supported by the provider.[5] PaaS is middleware, which can include access/identity/authentication management; specific vendors of PaaS include “Force.com, Google, AppEngine and Coghead.”[6] One specific beneficial use of PaaS is the development of standardized software programs.

Platform as a Service cloud computing companies are:

A. Google AppEngine is a development platform based upon Python and Java.

B. Salesforce.com's offers a development platform based upon a proprietary programming language called Apex.

C. Microsoft Azure provides a development platform based upon .Net.

2.3 Software as a Service (SaaS)

SaaS allows a customer to rent software applications provided over the Internet via a thin client/web browser (user does not own or control the infrastructure, servers, operating system, or storage); specific SaaS vendors include “Salesforce.com, Google Apps, and Oracle on Demand.”[7]

Software as a Service companies are:

A. Google offerings in the SaaS space include Google Docs, Gmail, Google Calendar and Picasa.

B. IBM provides LotusLive iNotes, a web based email service that provides messaging and calendaring capabilities to business users.
C. Zoho has vast suite of online products similar to Microsoft office suite.

3. Issues in Cloud Computing

3.1 Security related issues[8]

There are numbers of issues in cloud computing but some of the most important are presented below:

1. Data Centre security: It is important that every CSP (Cloud Service Provider) ensures their systems are secure in compliance with the current state of the technology. This includes permanent monitoring of access and fire protection precautions mechanism.
2. Server security: The operating systems deployed on the servers should be hardened to the extent that they offer the smallest possible area to attack. To achieve this, when the basic installation is being undertaken, only the necessary software packages should be added and any superfluous programs and services should be disabled or, better, uninstalled.
3. Network security: In the past, Cloud Computing platforms have often been misused either by placing malware there which is then used to send spam, or their processing power has been exploited to crack passwords using brute force attacks or to hide command and control servers (C&C servers) used to control botnets. To prevent these and similar attacks as well as the misuse of resources, each CSP should take effective security measures to defend against network-based attacks. As well as the usual IT security measures such as anti-virus protection, Trojan detection, spam protection, firewalls, Application Layer Gateway and IDS/IPS systems, and particular care should be taken to encrypt all communication between the CSP and the customer and between the provider's sites.
4. Application and Platform security: Security issues need to be addressed at each phase of the software development process in case of PaaS, and programs and modules may only be deployed if they have been properly tested and approved by the CSP's security manager. While software developed by the customer requires a secure basis (to be provided by the CSP), security issues also need to be considered in this respect. It is recommended that the CSP provides appropriate user guidelines for customers to create secure applications so that the programs the customer develops themselves fulfill certain minimum requirements in terms of security, documentation and quality.
5. Data security: The data life cycle comprises its generation, data storage, data usage, data distribution and data destruction. Each CSP should support all these phases in the data life cycle with appropriate security mechanisms. A number of storage technologies, e.g. NAS, SAN, Object Storage, etc., are used to store data. To avoid data losses, each CSP should do regular data backups based on a data security plan. Technical defects, incorrect parameterization, obsolescent media, inadequate data media administration and non-compliance with regulations stipulated in a data security plan can result in an inability to reinstall backups and reconstruct the data inventory.
6. Encryption and key management: To be able to store, process and transport sensitive data securely, suitable cryptographic methods and products should be used. The management of cryptographic keys in Cloud Computing environments is complex, and there are currently no appropriate tools for key management. For this reason, most providers do not encrypt data categorized as 'at rest'. The following key management best practices should be implemented:

   Keys should be generated in a secure environment and using suitable key generators.

   - Where possible, cryptographic keys should be used for one purpose only.
   - In general, keys should never be stored in the system in a clear form, but always encrypted. Furthermore, the storage should always be redundantly backed up and restorable, to avoid losing a key.
   - The keys must be distributed securely (on the basis of confidentiality, integrity and authenticity).

- The cloud's administrators should have no access to customers' keys. Keys should be regularly. The keys used should be regularly checked to ensure they are current.
- Access to key management functions should require a separate authentication.
- The keys should be archived securely.
- Keys that are no longer required (e.g. keys whose validity duration has elapsed) should be deleted or destroyed in a secure manner. Adequate cryptography skills are required for reliable key management. For this reason, CSP personnel who are responsible for key management must be identified and trained.

3.2 Issues in Application development

As cloud provider has no binding to follow the standard. So following are criteria for developers:

- Developer has to study the provider development tool kit.
- Developers must have the depth knowledge of language as well as the markup language supported by provider's tool to design and develop.
- Developers must have the depth knowledge of scripting language supported by provider's tool because event handling code should be browser free.
- Developers must have the depth knowledge of database server knowledge supported by provider's tool.
- Developers must have the depth knowledge of design pattern followed by provider's tool.

That is development language, scripting language, database server knowledge and design pattern may vary provider to provider. We cannot choose them.

3.3 Key Issues in the development life cycle

- System feasibility: Identify the security requirements, policies, standards, etc., that will be needed.
- Software plans and requirements: Identify the vulnerabilities, threats, and risks. Plan the appropriate level of protection. Complete a cost-benefit analysis.
- Product design: Plan for the security specifications in product design (access controls, encryption, etc.).
- Detailed design: Design the security controls in relationship to the business needs and legal liabilities.
- Coding: Develop the security-related software code and documentation.
- Integration product: Test security measures incorporated into software and make refinements.
- Implementation: Implement security measures and software and test before "going live."
- Operations and maintenance: Monitor security software for changes, test against threats, and implement appropriate changes when necessary.

4. Proposed Solution for Cloud Computing

4.1 Manage the basic security steps

The basic security steps are authentication, verification and validation of any application.
Authentication: All sites should have the following base password policy:

- Passwords must be 8 characters or greater
- Passwords must require letters and numbers
- Blacklisted passwords should be implemented (contact infrasec for the list)

Critical sites should add the following requirements to the password policy:

- Besides the base policy, passwords should also require at least one or more special characters.

Password rotations have proven to be a little tricky and this should only be used if there is lack of monitoring within the applications and there is a mitigating reason to use rotations. Reasonsbeing short password or lack of password controls.

- Privileged accounts - Password for privileged accounts should be rotated every: 90 to 120 days.
- General User Account - It is also recommended to implement password rotations for general users if possible.
- Log Entry - an application log entry for this event should be generated.
- Validation: Good Input Validation Approaches For each field define the types of acceptable characters and an acceptable number of characters for the input
- Username: Letters, numbers, certain special characters, 3 to 10 characters
- First name: Letters, single apostrophe, dash, 1 to 30 characters

- Simple US Zip code: Numbers, 5 characters

4.2 Enforcement of legality

To enforce the services of cloud computing globally there should be a global legal entity such as a global collaboration of CSP or a non-profit organization or Government of the particular country which can monitor the legal inequalities and standards among the CSPs. There should be one legal standard among the CSP around the world that will ensure transparency among the prospective users of cloud space/cloud computing. Thus, enforcement of legal standard will be beneficial both for the CSPs and users. Where CSPs can have pre-defined term and condition according to the standard legal agreement and the users can claim if he/she found any in equality in the legal standard of CSPs

4.3 Enforcement of Technical standard

Enforcement of Technical Standards in cloud computing related with information exchange, data portability and user authentication has not been standardized till date. This technical insecurity creates uncertainty in the mind of users/buyers. Working over cloud space provided by CSP created information exchange highway between cloud space and users that require authentication of users by the cloud space, this authentication process ensure the originality of the actual user of particular cloud space. Apart from the information related issues, CSPs should also standardize software application development platform. That mean user should not be restricted to choose from listed Software application platform provided by CSPs, hence the platform should be OPEN. Thus, the group of worldwide CSP should ensure and enforce standard technical authentication processes that insure data security, transparent working procedures over cloud, data portability from and to the cloud, data updating process and free from restricted number application development platform.

4.4 Enforcement of pricing policy

There are different types of CSPs and they provide a range of different cloud services with different technical advantages. The basic infrastructure such as hardware/physical space, leased high speed internet facilities, basic software to run the cloud hardware, user interface and the basic securities are almost identical for all the CSPs. Hence considering theses infrastructure, the pricing structures offered by the CSPs are not standard and there are huge inequalities over pricing decisions. Thus, there should be one governing council/group from the CSPs that ensure a range pricing structure for different cloud infrastructure and cloud application. The range of pricing policy will ensure proper growth and healthy competition among the CSPs mean while it also provide users to choose best option among the CSPs.

5. Conclusions

In fact cloud computing is not a new technology. We are using it since last ten years as “Gmail”. But now, it comes in market as “cloud computing” due to market demand. It is popular due to low cost and no maintenance charges or free of cost. It is good for small organization due to low cost. Its cost increase as number of users increases. We cannot predict its future due to security issues and cost for big origination. So, we have to follow the wait and watch policy. Each and every application can be categorized in three categories:

1. Business standard (which follow ISO standard)
2. Technical (Which follow standard Protocols)
3. Legal (Which follow Law enforcements and handling of cost)

But Cloud provider may be anyone having there infrastructure worldwide they may or may not follow these discussed issues because there are no authority to handle the cloud provider worldwide.

Cloud computing is broken down into three segments: "application" "storage" and "connectivity." Each segment serves a different purpose and offers different products for businesses and individuals around the world. In June 2011, a study conducted by Version One found that 91% of senior IT professionals actually don't know what cloud computing is and two-thirds of senior finance professionals are clear by the concept,[9] highlighting the young nature of the technology. In Sept 2011, an Aberdeen Group study found that disciplined companies achieved on average a 68% increase in their IT expense because cloud computing and only a 10% reduction in data center power costs.[10]

Thus the above survey also support our findings that modern cloud computing comprising “Application”, “Storage” and “Connectivity”, exists only when we have a International standard of business, legal and Technical procedure,.

Acknowledgments

We would like to thank Dr D.B. Ojha of Faculty of Engineering and Technology, Mewar University for encouraging us to write this paper.

References

[1] Interxion Cloud Survey http://www.interxion.com/cloud-insight/index.html

[2] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1

[3] Wald, "Cloud Computing for the Federal Community

[4]Mel Beckman, "Cloud Options that IT will Love," An Interactive eBook: Cloud Computing,July15,2010,at: http://www.networkworld.com/whitepapers/nww/pdf/eGuide_cloud_5brand_final.pdf

[5] Bret Michael and George Dinolt, "Establishing Trust in Cloud Computing," Information Assurance Newsletter, Vol. 13, No. 2 (Spring 2010).

[6] 30 Allan Carey, "Cloud Assurance Still Missing," Information Assurance Newsletter, Vol. 13, No. 1 (Winter 2010), 34.

[7] Ibid.-

[8]https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile

[9] C.D.K.Cook, B.J. Gupta, E.M.Rix, J.Scheller, and M.Serrz, Water plants of the world, Jurh, The Hague. Court, A. B. (1957),Sundry notes on three Victori, 1974.

[10] Business Adoption of Cloud Computing. AberdeenGroup (Sept 9, 2011).

First Author Shiv Kumar is currently doing M.Tech in (Computer Science and Engineering) from FET, Mewar University. His interest areas include cloud computing.

Second Author Bimlendu Prasad Verma is currently doing M.Tech in (Computer Science and Engineering) from FET, Mewar University and is a Member of IEEE. He is a keen contributor in forums like CodeProject, ExpertExchange, and Microsoft Technet. His interest areas are Document formats, Print Rendering and Document Management Systems

Third Author Archana Neog is currently working in Societe Generale of Banglore office as software engineer.