A Survey on Challenges of Integrating Web Service in Cloud Computing

Poornima Nedunchezhian
PG Scholar,Department of computer science and engineering,
Anna University of technology, Coimbatore,India.

Vidhyasree Venkatesh Moorthy
PG Scholar,Department of computer science and engineering,
Anna University of technology, Coimbatore,India.

Palanikkumar Durai Thirunavukkarasu
Assistant Professor,
Department of computer science and engineering,Anna University of technology,Coimbatore,India.

ABSTRACT

One of the most emerging techniques now a day is web service. The web service (WS) is provided by an international standard called World Wide Web Consortium (W3C). The communication between the systems in the network is enhanced by this service. Cloud computing (CC) provides better improvement in the functionality of WS. The CC hides the complex information's such as storage, network, and host details from the customers and gives easier environment to work. Even though several systems such as Amazon EC2, Microsoft Azure, and Google Application Engine (GAE) etc have evolved over time .They have its own challenges and issues. This survey gives an overview regarding some issues in cloud computing.

General Terms

Cloud computing, Web services.

Keywords

Simple Object Access Protocol (SOAP), Linux Apache MySQL PHP(LAMP), Security Assertion Markup Language (SAML), Human to Computer Interface(HCI), Quality of Service (QoS).

1. INTRODUCTION

The WS increases the network capacity [11] and provides good differential services. This service manages network traffic, QOS. The QOS can be measured technically or with business attributes. The representation of CC resembles network representation in telephone network. The CC in the WS provides easier API to customers. This drag the customers towards the WS using CC.

1.1 Overview of CC

Figure1 represents the interaction between web service provider and customer, who access the WS via web browser (e.g.: Mozilla Firefox, Internet explorer, Google chrome etc).the Web browser access the web service provided by the CC through internet. Every CC has its own application platforms, service providers and software. The SQL is used to access the DB in the CC environment. The customer request WS5 from service provider, then the provider selects the requested WS5 alone from the set of N WS.

1.2 Layered CC

Figure2 shows the function inside the layers of CC. At layer1 multitenant software is implemented. Layer2 gives a template or framework for building application to the developers.

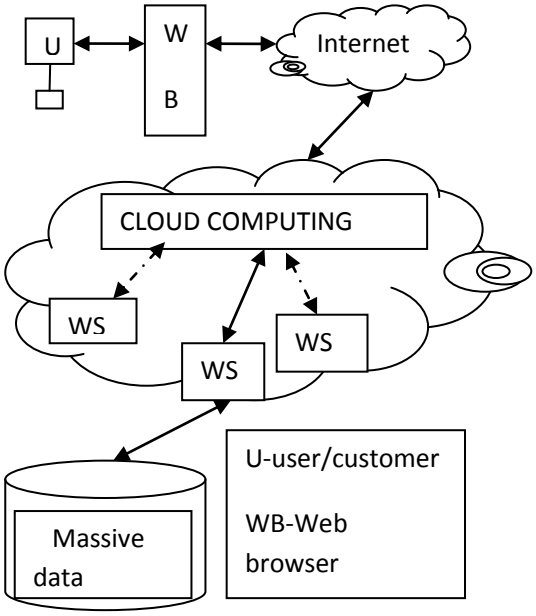

Figure 1 Flow architecture of Cloud Computing.

There are up to date technologies in layer3 the user can choose the apt one for faster service.This is referred as on demand access. In layer 4 the data centers prevails which reduces the cost of developing and organizing the cost of application.

1.3 Features of Cloud

The multitenancy [8] is one of the most important feature in CC.

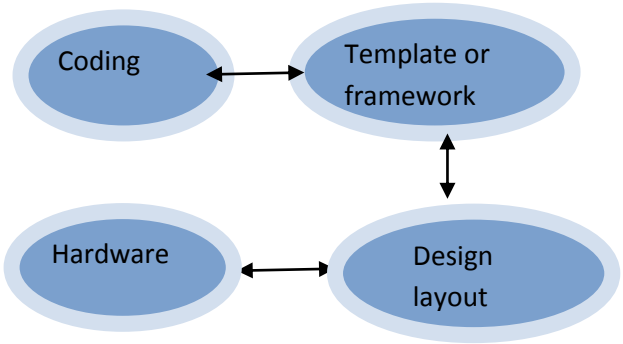

Figure2 stages of cloud computing

Here more than one user uses same software at least cost. The CC can hold large volume of data hiding the difficulties to the customers and pretend as a simpler system. Storage, server.Virtualization helps to avoiding complexity.

Interoperability offers communication between various platforms the resource sharing is possible here so resource optimization can be done.

1.4 Risk Factors

In Figure 3, the energy consumption is high due to virtualization [3] of storage server etc. The privacy [6] is the greatest problem in CC. Since the customers are unaware of the location of their data stored and thus they lack control over the data.

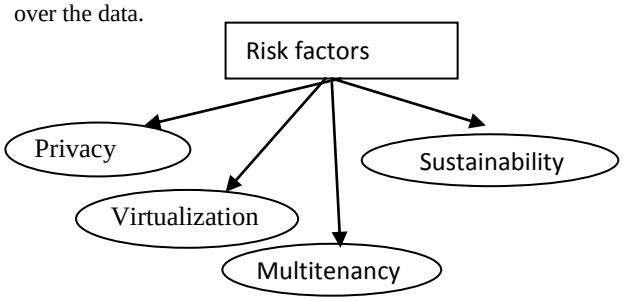

Figure 3 Issues in cloud computing.

The third party handles the user data in CC environment. So, there is no assurance of privacy of user data. There is no common standard in CC. hence one vendor application need not be compatible with other vendors. Based on the access internal/external the clouds are categorized as: public, community, private, and hybrid clouds.

2. MONITORING EXAMPLE

Figure 4 shows in CC each system has cloud based architecture. The integration of departments in college is motivating example. The university acts a cloud. They have several departments e.g. CSE (computer science and engineering). Each department acts as autonomous cloud. They have both sensitive and non sensitive data. The sensitive data is private and accessed only by authorized or internal user. The server within the clouds has control over the data. The non sensitive data is accessed by public users. Each department inside the college cloud can act as internal cloud.

The department of CSE can able to access sensitive information of EEE because all these departments are integrated. The database is used to store and retrieve the sensitive data of the college which cannot be accessed from the public clouds. The authentication monitoring system authenticates the information from intruders by checking the authority of user. If the authority of the user is valid then it is able to access the information from database else it is considered as third party and denies service. This denied request thrown to thrash. The authentication monitoring system is responsible for controlling all the internal clouds inside college. The request from other public clouds is also discarded. So the privacy is ensured.

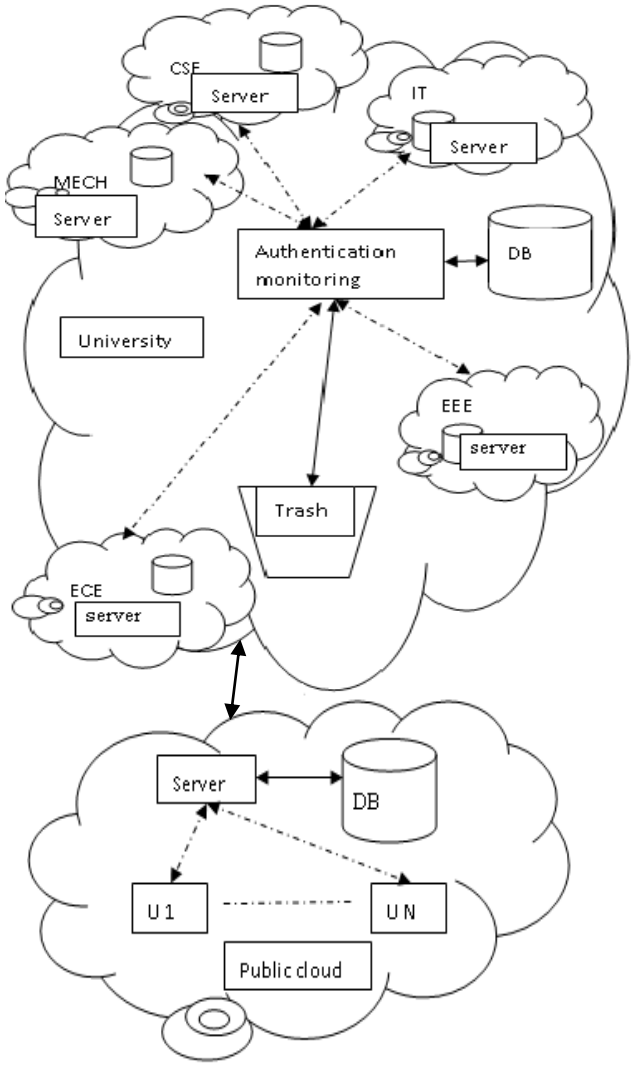

Figure 4 integrating the department within the college.

3. CHALLENGES AND ISSUES

The taxonomy of CC [1] says the cloud development is based on vendors only and not based on IT. The CC performs its computation in a distributed environment for e.g. Google handles bulk data. The fault tolerance in CC is achieved by the backup of data. The user should have control over data. The lack of this control leads to several problems as: malfunction programming error, site unavailable due to outages in contact system; core network failure etc. to improve the service, one has to overcome all the outages e.g. Military application – encryption/ decryption details resides with authority.

Seven standards [2] for CC help to reduce cost and time consumption. The top service provider vendors is in demand e.g.salesforce.com, recommends 7 standards to be followed in every cloud based systems for resource sharing and highest service delivery, they are: world class security, trust and transparency, true multitenancy, high performance , complete disaster recovery, proven scale and high availability.

Emantra [3] is provider of cloud service. Iaas (Infrastructure as a service) gives service based on virtualization. Paas (Platform as a service) uses SQL. RDP (Remote Desktop Applications) accesses the data and applications from the remote computer. The security in the internet is the vital feature. The malicious programs can affect the system and cause security issues. It is not necessary for the system to get

connected in internet always instead PCFC [4] (private cloud file characteristic) is used. The private cloud is accessing the data within its own cloud. PCFC provides authentication. The sensitive data is retrieved only by the private members of the cloud. The authentication engine after receiving the request will check for its privacy. Malicious programs can also infect file. To scan a file it is not necessary to send the entire file to authentication engine, only the security characteristics are needed.

In distributed environment the cloud auditing [5] is difficult. The cloud development is done in two ways simply using cloud service provider and open source software e.g. Apache, MySQL and LAMP. The data is organized as profiles (tables). The data access is done by XACML (extensible Access Control Markup Language).

Figure 5 shows trust management is the combination of privacy and security policies [6]. The applications are build on platforms which contains database, network, host. The privacy should be given for user data. Security is implemented in every layer of development cycle of sales force.com. The security monitoring is used to monitor the threads and intrusions'.

The data in the cloud environment is categorized as sensitive and non sensitive data [7]. The sensitive data can be stored in private cloud. The full control of sensitive data resides with the customer. The authentication monitoring system restricts the access from public cloud.

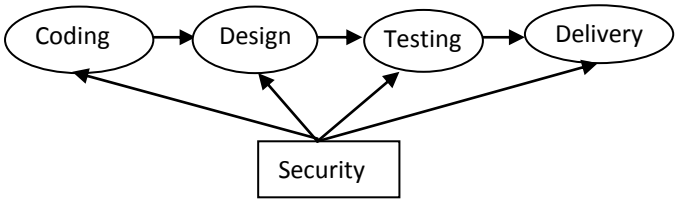

Figure 5 Secure and private trustworthy system

The location of non sensitive data is not known to the customer and probably has no control. These of data emerged due to the privacy issue of organizing the overall raw data by third party.

Multitenancy [8] allows multi users to work on a virtual platform. The problems in multitenancy are encryption and homomorphic encryption. The same encryption algorithm is used on all users' data. The Aspect Oriented Functionality (AOP) separates the security function from core function.

HCI (human to computer interface) [9] customize the application building and storage. The storage, data, cloud are directly propotional.The two fields of interactive design are interface design, service design (telephone service).In framing the issues of CC and sustainability icloud (interactive cloud)is the programming language that provides first class design for interaction. The interaction between cloud service and application are programmable.

So, it needs fundamental knowledge related to the program. The supreme solution for the security issue is auditing [10,5]. The audit process is performed at runtime and checks for security. In organization the auditing checks in data storage whereas for users the assurance of data security is needed.

The auditing cannot be done by the customers, it relies on third party. So there is a threat for information leakage. The versioning of auditing is done through public auditing, batch auditing and challenge response auditing protocols.

1. The public auditing system

The algorithms are used to assure the data security since the third party is unaware of the content during auditing.

2. Batch auditing system

The auditing process is done for more than one user simultaneously.

3. Challenge response auditing protocol

The data integrity is provided the fraudulent customers are also found out

TPA (Third Party Auditing) can be automated to reduce security issue.

All the implementation in CC [12] is based on its layers. Iaas is a open source that offers several criteria such as storage, virtualization, management, security, network and vendor. The backup is the most important feature in storage criteria. Each virtualization product has their unique features. So the commentary must be provided in these products. The access of virtual machine and its management is given by network criteria.

The products are evaluated based on how the system is managed through clouds offered by management criteria. The features of each system depend on how the product manages the cloud based application. IGF (Integration Group Focus) [12] provides the interaction between software, hardware, and host and network application. The cloud system reports to the user the amount of resource used, data collected and network details. If the system gets affected through any malfunction it alarms to the user. To recover the data recovery management is used.

The virtualization, storage, network management depends on the implementation of the cloud. The security provides authentication, authorization and reports the user by auditing. The product for grading uses the numerical ranging methods. This helps to identify the product quality. There may be many CC solutions such as Abiquo community edition, Eqcalyptus community cloud (ECC), Nimbus, MOSAIC, Open Nebula etc.

The system architecture [13] for private cloud monitoring has view layers which administrates the network and perform a other managing process. The integration layer is sandwiched between the view layer that perform information gathering and configuration. The infrastructure layer has several structures that are inbuilt and acts as a format for building applications. The private cloud can have several clusters within its body.

Each cluster has PCMONS (Private Cloud Monitoring) modules. All the cluster data are combined are by a cluster data integrator which has the database and its organization is by admin, manager. The virtual machines are directly attached to the private cloud. The monitoring tool used here is virtual machine monitor.The administration in a virtual machine is same as the clusters. The user can access the clusters (sets of nodes) with application programming interface (API). There are several open source CC platforms [14] such as XCP (Xen cloud platform), Eucalyptus, and Open Nebula. In XCP architecture the private network has several XCP host and master XCP host commands the individual host in a network. The shared storage stores the virtual machine images for administration. The network architecture connects virtual machine to an Ethernet by virtual Ethernet switch (VES) and physical network interface. The interface between the virtual Ethernet switch and Ethernet switch is virtual interface. The Eucalyptus has cloud controller and storage controller (walrus) which is connected to a cluster controller in a public network. The cluster controller controls over the node controller in a private network. The cluster controller and node controller are the components of the clusters.

The privacy issues [15, 18] for CC are sensitive. Every individual differs in their personal information and the sensitive data differs from one to other. The following are few

sensitive data: the personally identified information stores the individual's information. The sensitive information are based on race, politics etc.

The data are retrieved/stored from computers for users' purpose such as printer/scanner. The history in web browser is the example of usage data that should be protected from intruders. Every device has unique identity. This identity is used by the intruders to track the device to protect the sensitive data. The engineers when designing should minimize the storage of sensitive data in public cloud and the maximization of user cloud id recommended.

The service level agreement (SLA) [16] assures the quality of service. This is signed between the customer and service provider. Any web service incorporated with CC needs good service. To check the level of service a checker is used which compares the target framework with SLA as a input. This generates the service level compliance results.

This feedback helps the provider to improve service. The architecture of service level compliance is service monitoring, data collector and core monitoring. The core monitoring is the last layer that interacts with software and hardware. It collects the data from several nodes. The service monitor checks for Service Level Agreements (SLA). The result of SLC may be SLA compliance or its failure.

In cloud computing there are many data centers [17] in cloud environment. Each data centre has several physical servers. Several virtual machines are embedded inside physical server. There is a legal jurisdiction who manages several virtual machine in all data centres.The virtual machine can also migrate from one data centre to other or within itself.

The cloud threats [19] due to security issue can be effectively managed. This issue is when the application is running or closer to the public cloud.Ramgovind has surveyed Gartners list from international data corporation enterprise panel. The cloud computing is used mostly by the people seeking for faster results. The SLA is given by the service provider to the clients. The Iaas is a paper usage shares the resource within the cloud computing members' .In Saas the software is rented only to their members under contract. This software can be versioned for enhancement. The platform building is costler and it also rented to the users. The auditing is used for checking tags which is one of the embedded cloud securities. In web security the simple objects access protocol (SOAP) message can be used.

The Iaas [20] providers the user with CPU, storage enhancement functions. All these are governed by Iaas provider. In Paas the user can custom their own application and also check and correct for errors.

The Saas depends on a browser for accessing/retrieval of data centers e.g. salesforce.com and zoho. The architecture has three designs [20]

i. Replication of Application
   The user is allowed to compare the application with others available in the internet showing the efficiency of the application.
ii. Partition of application system into tiers
   This stores the core concept of application into a cloud separately. These reduce faults in real time application.
iii. Partition of application tier into fragments
   This partitions the data in to confidential and non-confidential data and restricts the access to the confidential data. To avoid threats regarding data storage the single application can be split up into several fragments (app1, app2, app3, app4,….,appN) for easy organizing by fragmenting the application the computation on the system is fragmented.
   Several parties can be used for the purpose of auditing and computation

The grid computing [21] has vertical and horizontal of nodes in physical implementation. This divides bulk application to several small applications and runs them in simultaneous and concurrent fashion. The output of a small application can be a feed back and as given as a input to other smaller application. There are several roles for the users that affect grid computing system by data leakage/modification, data/platform sharing, accessing methods.

In web service there are cloud and non-cloud platforms. The cloud computing is closely related to the characteristics of grid based computing, autonomous computing, utility computing, mainframe computing etc.

The autonomous computing is a standalone computing environment which uses its own application and does not depend on others. The utility computing based on usage criteria(pay-per-usage system) .The mainframe computing system handles larger applications such as census system, server admin etc.

In the trust network [22] the identity provider and cloud service provider which have the authentication services and auditing functions etc. Inside a network there are many WS clients waiting for trust and reputation service. The dash board service is offered for users.All the trusted services are aggregated by trusted attribute aggregator service. The service directory maintains all the request, acceptance, denial and processing information.

When the client request the server the job scheduling is performed. The scheduling is static or dnamic in nature. The scheduling [23] sytems can be centralized/ decentralized. The execution time of each task is predicted using predicted execution time module. The scheduling optimizer performs fuzzification and scheduling. The failure of the scheduling can be recovered by rescheduling.

4. CONCLUSION

Several web service techniques are using cloud computing technique to provide their customers easy interface. Even though many systems prevail it has no standard framework. There occur several issues/challenges in integrating the cloud computing in web service. These issues cannot be totally recovered but can be reduced it some extent by implementing the cloud computing standards. Each cloud computing technique such as auditing, segregation, fragmentation and replication of application, service level aggrement checking, and remote desktop protocol (RDP), human to computer interface are used to reduce the issues.

5. REFERENCE

[1] Bhaskar Prasad Rimal , Eunmi choi, Ian Lumb,"A taxonomy and survey of cloud computing systems", 2009 fifth international joint conference on INC, IMS and IDC.

[2] Salesforce.com,"The seven standards for cloud computing service delivery.

[3] www.emanthra.com.au/cloud-menu/cloud-tco.

[4] Xuesen Lin, "survey on cloud based mobile security and a new framework for improvement", preceeding of IEEE

international conference on information and automation Shenzhen, china june 2011.

[5] Aiiad Albeshri and William Caelli, "mutual protection in a cloud computing environment", 2010 12th IEEE international conference on high performance computer and communication.

[6] Sales force.com, "secure, private, and trustworthy: enterprise cloud computing with force.com".

[7] Chhand Ray, Uttam Ganguly, "An approach for data privacy in hybrid cloud environment", international conference on computer and communication technology (ICCCT)-2011.

[8] Katie Wood, Dr Mark Anderson,"Understanding the complexity surrounding multitenancy in cloud computing", 2011 8th IEEE international conference on e-business engineering.

[9] Yue Pam, Siddharth Maini and Eli Blevis, "Framing the issues of cloud computing and sustainability: A design perspective" 2nd IEEE international conference on cloud computing technology and science.

[10] Irfan Gul,Atiq ur Rehman, M. Hasan Islam,"Cloud computing security auditing".

[11] Runtong Zhang, Yannis A.Phillis, and Jain Ma,"A fuzzy approach to the balance of drop and delay priorities in differentiated services networks"IEEE transcation on fuzzy systems, VOL. 1, NO.6, December 2003.

[12] Ivan Voras, Branko mihaljevic, and Marin Orlic,"Criteria for evaluation of open source cloud computing solutions".

[13] Shirlei Aparecibа et al.,"Topics in design and implementation:Toward an aarchitecture for monitoing private clouds"

[14] Thiagocor cordeiro, Douglais et al,"open source cloud computing platforms"2010 9th international onference on grid and cloud computing.

[15] Siani Pearson "Taking account of privacy when desiging cloud computing services"cloud 09 may 23, 2009 Vancouver, Canada 2009 IEEE.

[16] Antonin Chazalet, "Service level aggrements compliance checking in cloud computing" 2010 5th international conferences on software engineering advances.

[17] Brianjay, Kra Nance, Matt Bishop, "Strom clouds rising: Security challenges for Iaas cloud computing" preceedings of the 44th hwaii international conferences on system sciences-2011.

[18] Karesimir Popovic, Zelzko ho Censki,"colud computing security and challenges"MIPRO 2010, may24-28 2010 OPATIJA, CROATIA.

[19] Ramgovind S, Eloff MM Smith E,"The management of security in cloud computing",2010 IEEE.

[20] Meiko Jensen, Jorg Schwenk Jens, Matthias Bohli, Nils Gruschka Luigi Lo Iacomo, "Security prospects through cloud computing by adapting multiple clouds", 2011 IEEE 4th international conference on cloud computing.

[21] Yogesh Simmhan,Alok Gautan Kunbhare, Baohua Cao and Viktor Prasanna, "An analysis of security and privacy issue in smart grid software architecture on clouds" 2011 IEEE 4th international conference on cloud computing

[22] David W Chadwick, Stijin F Lievens Jerry I Den Hartog, Andreas Pashalidis, Joseph Alhadeff,"My private cloud overview" 2011 IEEE 4th international conference on cloud computing.

[23] Sandeep Tayal, "Task schedling optimization for the cloud computing systems", IJAEST VOL NO.5 issue No.2 111-115.