ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 4, Issue 12, December 2017

Cloud Computing - Web Services

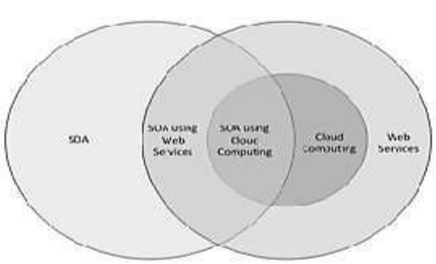
Abhirati Ghosh

MBATech IT 3rd year, Mukesh Patel School of Technology and Management, NMIMS, Mumbai

***Abstract*— Today's models and systems (in the application approach) are used according to the user's needs, while the rest of the time computing resources remain not used. Such services are characterized by extremely high level of security and synchronization of files that are continuously exchanged. Cloud computing is an information technology paradigm, a model for enabling ubiquitous access to shared pools of configurable resources, which can be rapidly provisioned with minimal management effort, often over the Internet. A web service is a service offered by an electronic device to another electronic device, communicating with each other via the World Wide Web. This paper links between the two.**

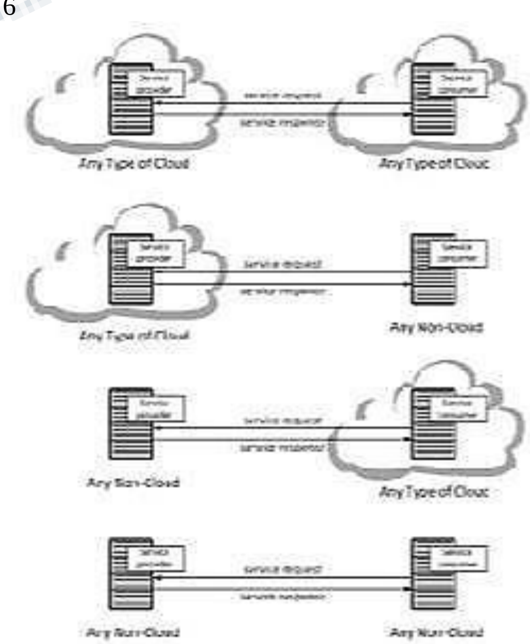
I. INTRODUCTION

With the rapid development of information technology we see a strong ongoing need to improve the current state of information systems in education. Cloud computing or cloud technology is the answer that fulfill the above mentioned need in order to increase the capacity and provide new features on the existing infrastructure without investing in new infrastructure and personnel. This technology has enabled customers to use computing resources using only a web browser (e.g. Internet Explorer, Chrome or Firefox) thereby using the existing computing resources. Cloud technology is a kind of technology mainly oriented to end users and is implemented through a number of services like providing additional disk space, memory and network capacity as well as providing quality free software applications. The following Venn diagram illustrates the relationships among Web Services, service-oriented architecture (SOA), and Cloud Computing. Web Services encapsulates Cloud Computing in this diagram because Cloud Computing use Web Services for connections (you might find exceptions, but they are rare). It is possible, however, to use Web Services in situations other than Cloud Computing. Such use of Web Services may be part of a service-oriented architecture, but it may not. Web Services could be simply be a connection. Finally, it is possible to have a service-oriented architecture and not use Web Services for connections



II. ARCHITECTURE

Applications must manage all resources of Cloud Computing infrastructure in order to ensure quality services to end users (students). Applications are to be developed for various platforms: Android mobile platforms, Linux, windows and other. The applications would depend on existing Cloud Computing infrastructure, and would be integrated with the root computer of end users (LDAP) which contains accounts for access and relies on web services, what allows future development of other applications that have similar purposes and capabilities. Through the comparable method, a similar application would be developed as well as the web applications with the same purpose. The application would primarily benefit students chosen to conduct the research experiment, which would allow them to schedule and run predefined virtual machines with all the 6



ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

installed operating systems and necessary software that is required for the particular course. The software application would use the service-oriented architecture, which allows comparative development of web and mobile applications. The mentioned approach to software development would lead to the creation desktop applications and integration with more some existing system.

A. Software as a Service (SaaS)

Cloud consumers release their applications in a hosting environment, which can be accessed through networks from various clients (e.g. Web browser, PDA, etc.) by application users. Cloud consumers do not have control over the cloud infrastructure that often employs multi-tenancy system architecture, namely, different cloud consumers' applications are organized in a single logical environment in the SaaS cloud to achieve economies of scale and optimization in terms of speed, security, availability, disaster recovery and maintenance. Examples of SaaS include SalesForce.com, Google Mail, Google Docs, and so forth.

B. Platform as a Service (PaaS)

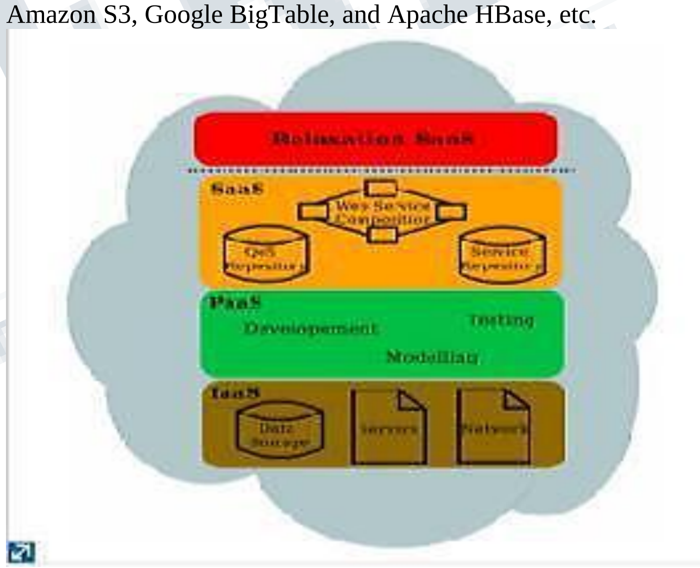
PaaS is a development platform supporting the full “Software Lifecycle” which allows cloud consumers to develop cloud services and applications (e.g. SaaS) directly on the PaaS cloud. Hence, the difference between SaaS and PaaS is that SaaS only hosts completed cloud applications whereas PaaS offers a development platform that hosts both completed and in-progress cloud applications. This requires PaaS, in addition to supporting application hosting environment, to possess development infrastructure including programming environment, tools, configuration management, and so forth. An example of PaaS is Google AppEngine.

C. Infrastructure as a Service (IaaS)

Cloud consumers directly use IT infrastructures (processing, storage, networks and other fundamental computing resources) provided in the IaaS cloud. Virtualization is extensively used in IaaS cloud in order to integrate/ decompose physical resources in an ad-hoc manner to meet growing or shrinking resource demand from cloud consumers. The basic strategy of virtualization is to set up independent virtual machines (VM) that are isolated from both the underlying hardware and other VMs. Notice that this strategy is different from the multi-tenancy model, which aims to transform the application software architecture so that multiple instances (from multiple cloud consumers) can run on a single application (i.e. the same logic machine). An example of IaaS is Amazon's EC2.

D. Data as a Service (DaaS)

The delivery of virtualized storage on demand becomes a separate Cloud service - data storage service. Notice that DaaS could be seen as a special type IaaS. The motivation is that on-premise enterprise database systems are often tied in a prohibitive upfront cost in dedicated server, software license, post-delivery services and in-house IT maintenance. DaaS allows consumers to pay for what they are actually using rather than the site license for the entire database. In addition to traditional storage interfaces such as RDBMS and file systems, some DaaS offerings provide table-style abstractions that are designed to scale out to store and retrieve a huge amount of data within a very compressed timeframe, often too large, too expensive or too slow for most commercial RDBMS to cope with. Examples of this kind of DaaS include Amazon S3, Google BigTable, and Apache HBase, etc.



III. CLOUD COMPUTING GOVERNANCE

A. Technical Issues

Determine how the Cloud Provider::

- Supports change management
- Provides for high-availability
- Provides for redundancy and failover (if any)
- Provides for security related to the Internet
- Provides for physical security

B. Legal Issues

It is important to determine what needs to be in a contract with your Cloud provider. Things to consider:

▪ Service standards to be maintained
▪ Retention of rights to your data
▪ Legal jurisdiction where the data center is located
▪ Privacy laws where the data center is located
▪ Liability of data breaches
▪ Policies and procedures related to providing digital forensics data in the event of any legal dispute, cyber attack, or data breach.
▪ Notification of changes when they occur at the data center
▪ Disaster recovery
▪ Remedies for various possible problems
▪ Details for what occurs at the beginning and end of the contract period

C. Business Issues

Your business relationship with a Cloud provider should involve:

▪ The Cloud provider's reputation
▪ Financial stability of the Cloud provider
▪ The length of time the Cloud provider has been in business

IV. ISUUES IN CLOUD COMPUTING

More and more information on individuals and companies is placed in the cloud; concerns are beginning to grow about just how safe an environment it is? Issues of cloud computing [3] can summarize as follows:

A. Privacy

Cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data centers rather than stay in the same physical location, users
may leak hidden information when they are accessed cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users may leak hidden information when they are accessed cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users.

B. Reliability

The cloud servers also experience downtimes and slowdowns as our local server.

C. Legal Issues

Worries stick with safety measures and confidentiality of individual all the way through legislative levels.

D. Compliance

Numerous regulations pertain to the storage and use of data requires regular reporting and audit trails. In addition to the requirements to which customers are subject, the data centers maintained by cloud providers may also be subject to compliance requirements.

E. Freedom

Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers.

F. Long- Term Viability

You should be sure that the data you put into the cloud will never become invalid even your cloud computing provider go broke or get acquired and swallowed up by a larger company.

G. Issues in Cloud Interoperability

1) Intermediary Layer

A number of recent works address the interoperability issue by providing an intermediary layer between the cloud consumers and the cloud-specific resources (e.g. VM).

2) Open Standard

Standardization appears to be a good solution to address the interoperability issue. However, as cloud computing just starts to take off, the interoperability problem has not appeared on the pressing agenda of major industry cloud vendors.

3) Open API

SUN has recently launched the Sun Open Cloud Platform [10] under the Creative Commons license. A major contribution of this platform is the proposed (in-progress) the cloud API. It defines a set of clear and easy-to-understand RESTful Web services interfaces, through which cloud consumers are able to create and manage cloud resources, including compute, storage, and networking components in a unified way.

4) SaaS and PaaS Interoperability

While the aforementioned solutions generally tackle with IaaS interoperability problems, SaaS interoperability often involves different application domains such as ERP, CRM, etc. A group of experts in the field of data mining

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

raises the issue of establishing a data mining standard on the cloud, with a
particular focus on "the practical use of statistical algorithms, reliable production deployment of models and the integration of predictive analytics" across different data mining-based SaaS clouds. PaaS interoperability not yet discovered Since PaaS involves the entire software development life-cycle on the cloud, it would be more difficult to reach the uniformity with regards to the way consumers develop and deploy cloud applications.

V. SECURITY AND PRIVACY ISSUE

Cloud computing can provide infinite computing resources on demand due to its high scalability in nature, which eliminates the needs for Cloud service providers to plan far ahead on hardware provisioning. Many companies, such as Amazon, Google, Microsoft and so on, accelerate their paces in developing cloud computing systems and enhancing its services providing to a larger amount of users.
In this paper, we investigate the security and privacy concerns of current cloud computing systems provided by an amount of companies. As cloud computing refers to both the applications delivered as services over the Internet and the infrastructures (i.e., the hardware and systems software in the data centers) that provide those services. Based on the investigation security and privacy concerns provided by companies nowadays are not adequate, and consequently result in a big obstacle for users to adapt into the cloud computing systems. Hence, more concerns on security issues, such as availability, confidentiality, data integrity, control, audit and so on, should be taken into account.

A. Security on Demand

Cloud services are applications running somewhere in the cloud computing infrastructures through internal network or Internet. Cloud computing allows providers to develop, deploy and run applications that can easily grow in capacity (scalability), work rapidly (performance), and never (or at
least rarely) fail (reliability), without any concerns on the properties and the locations of the underlying infrastructures. Cloud computing systems can achieve the following five goals together:

1) Availability

The goal of availability for cloud computing systems (including applications and its infrastructures) is to ensure its users can use them at any time, at any place. As its web-native nature, cloud computing system enables its users to access the system (e.g., applications, services) from anywhere. This is true for all the cloud computing systems (e.g., DaaS, SaaS, PaaS, IaaS, and etc.). Required to be accessed at any time, the cloud computing system should be severing all the time for all the users (say it is scalable for any number of users). Two strategies, say hardening and redundancy, are mainly used to enhance the availability of the cloud system or applications hosted on it.

2) Confidentiality

It means keeping users' data secret in the cloud systems. There are two basic approaches (i.e., physical isolation and cryptography) to achieve such confidentiality, which are extensively adopted by the cloud computing vendors.

3) Data integrity

In the cloud system means to preserve information integrity (i.e., not lost or modified by unauthorized users). As data are
the base for providing cloud computing services, such as Data as a Service, Software as a Service, Platform as a Service,
keeping data integrity is a fundamental task.

4) Control

In the cloud system means to regulate the use of the system, including the applications, its infrastructure and the data.

5)Audit

It means to watch what happened in the cloud system. Auditability could be added as an additional layer in the virtualized operation system (or virtualized application environment) hosted on the virtual machine to provide facilities watching what happened in the system. It is much more secure than that is built into the applications or into the software themselves, since it is able watch the entire access duration.

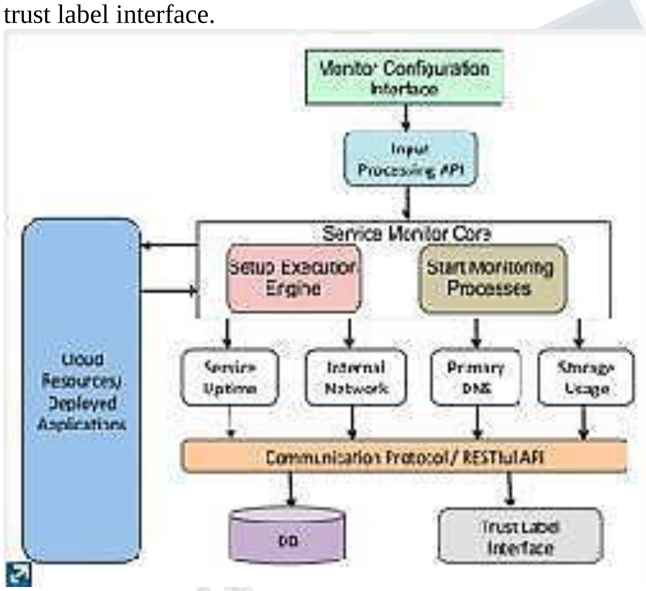
VI. SERVICE MONITOR FRAMEWORK DESIGN

The service monitor framework is a composite monitoring platform consisting of independent configurable monitoring tools that are managed in a decentralised manner. It is a holistic framework capable of monitoring both at the infrastructure and application levels in Clouds. Since many of the Cloud services today are application based, a resource-monitoring tool like LoM2HiS would not be capable of monitoring all aspects of such

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

deployments.
The service monitor framework consists of different components that work together to achieve its objectives. The Monitor Configuration Interface is the front-end component
for configuring the monitoring tools. It allows the parameterisation of the individual monitoring tools, for example to specify different monitoring intervals, and also the selection of particular monitoring tools for different purposes. The Input Processing API gathers the configurations created using the front-end component and parses them into a suitable format for the back-end service monitor core engine to understand. It is the responsibility of the Service Monitor Core to instantiate the necessary monitoring tools with the proper configuration parameters and to co-ordinate their execution while they monitor the Cloud resources and deployed applications. The monitoring tools are executed in parallel and each sends its monitored data using the communication protocol into a database as well as to the trust label interface.



VII. TRUST CHALLENGES AND RELATED WORK

The trust challenges raised by the emergence of Cloud computing are similar to those raised by the Internet at a whole. Consumers of Cloud computing, similar to general Internet consumers must trust that Cloud providers will deliver the agreed quality of service, securely store their data and respect their privacy. In the Internet, trustmarks, which are any third-party mark, picture or symbol, have been used in an effort to dispel consumers' concerns regarding risk and therefore increase their trust. Recipients of trustmarks are typically subjected to a manual verification and certification process that varies among the trustmark issuing sectors and is not transparent to consumers. Therefore, the approach is open to criticism regarding accuracy, consistency, timeliness, transparency and ease of abuse. Based on the static and passive forms of trustmarks, they cannot be effectively used to address the trust and confidence issues in Cloud computing due to the mostly dynamic nature of Cloud services. As a result, a more active and dynamic approach is required for providing trust information for Cloud consumers. The Cloud Security Alliance (CSA) Security Trust & Assurance Registry (STAR) is a method designed for providing security assurance certification in Clouds. It certifies and assures the compliance of Cloud provider security practices to consumers. Notwithstanding this, such assurance (and associated trustmarks) have been subject to criticism for being (i) largely reliant on human intervention (with limited capacity), (ii) limited in scope, (iii) passive, periodical and retrospective, (iv) lacking warranties and (v) subject to co-optation risk. More recently, CSA STAR is working to integrate continuous monitoring in an effort to alleviate some of those criticisms and to automate the certification process. This shows the importance of flexible monitoring for such systems and it clearly relates to our operationalisation approach in this paper for the trust label system, which covers a broader spectrum of Cloud service metrics other than security. The CSA CloudTrust Protocol (CTP) presents a similar mechanism for managing Cloud service security to improve consumer trust. However, security controls are only one part of the wider fabric that makes up trust and thus a security-oriented perspectives does not capture the wider complexity of how trust is formed, maintained or lost. The CTP API can be integrated with the trust label system to push security measurements to the label interface. However, further work would be needed to explore those security measurements and validate whether they in fact either build trust or contribute to trust and at what level. At the moment, there is an open question on how CTP could be consumed by consumers and enterprise buyers. We argue that it can be made consumable by integrating it with the trust label system.

IV. APPLICATION EXAMPLE

Based on the platform an integrated information system was developed. Using the cloud computing and the heterogeneous data integration technology, the comprehensive monitoring is provided to the personnel, vehicles and other entities. The comprehensive management information service is provided for users, in order to improve the level of information management. There are some integration methods in this system, such as the ESB, Web Service, the virtual database, etc. The 6 types, existing 21 business systems are integrated in order to unifiedly manage and dispatch the data and service resource. Using RIA technology, through the enterprise service bus, heterogeneous data integration technology, the polymerization, showing of all kinds of information is realized. In the integrated management information system, as shown in Figure, the main page displays vehicle information, real-time monitoring of vehicle information.

Compared with other similar systems, this system also has the following advantages: x Based on the cloud computing and Internet of things architecture, a flexible cloud computing is built to realize a flexible and robust framework. Not only can be used for the development and installation of a variety of service component on such framework and can realize the integration of third party applications. x Through a unified open business model, by a standard interface the software platform level services engine is provided to construct a modular, flexible, and scalable integrated application platform for the users.
x Based on the flexible customization technology business process model is developed to realize flow dynamic change, on-demand service module, dynamic deployment, application of dynamic reconfiguration. x Using a variety of comprehensive practical design, the system usability, visibility and standardization is improved.

VIII. CONCLUSION

In this paper we have discussed a new wave in the eld of information technology: cloud computing. We have also described its architecture, advantages and some issues. Each
approach has its concerns and a focus on certain aspects of an IT solution. With SOA, we can make managing cloud services implement and manage security policies and manage issues with business processes—concerns that are beyond the scope of Cloud Computing. The combination of both approaches allows the company to focus their efforts on more relevant issues to the business without giving adequate operation and without the organization losing flexibility in system maintenance equipment, while allowing flexibility in the creation of new features. Each of the presented approaches has values and utilities in different domains, as well as different problems. But the use of both is critical to maximize quality in all aspects of an IT solution, in view of their complementary characteristics to each other. As stated, Cloud Computing provides the infrastructure for an application and SOA architecture and methods to manage the remaining issues for implementing the solution. While it is possible to use either approach independently with reasonable results, both SOA and Cloud Computing offer several implementation possibilities, and their union is one of them. The use of this solution depends on the current situation of the organization, as well as the maturity of the business and the team involved in the migration of legacy systems. Due to the breadth of the subject, the aim of this paper was to obtain a reference that serves as a starting point to begin further study in order to minimize risks and problems in case of implementation of a SOA in the Cloud Computing model.

REFERENCES

1. https://www.service-architecture.com/articles/cloud-computing/web_services_and_cloud_computing.html

2. https://www.service-architecture.com/articles/cloud-computing/service oriented_architecture_soa_and_cloud_computing.html

3. http://www.ijfcc.org/papers/95-F0048.pdfK. Elissa, “Title of paper if known,” unpublished.

4. Y. Jadeja and K. Modi, "Cloud computing - concepts, architecture and challenges," 2012 International Conference on Computing, Electronics and Electrical

Technologies (ICCEET), Kumaracoil, 2012, pp. 877-880.

5. ”The NIST Definition of Cloud Computing, Special Publication 800–145", Peter Mell, Timothy Grance, Computer Security Division Information Technology Laboratory National Institute of Standards and TechnologyGaithersburg, Septembar 2011.

6. John Harauz, Lorti M. Kaufinan. Bruce Potter, "Data Security in the World of Cloud Computing", IEEE Security & Privacy, Copublished by the IEEE Computer and Reliability Societies, July/August 2009.

7. S. Reid, H. Kilster, "Sizing the cloud", 2011.

8. Web service model for distance learning using cloud computing technologies

9. Dragan Cvetkovic; Marko Mijatovic; Marijan Mijatovic; Branko Medic

10. 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics .

11.WANG Pei, JIANG Chao hui, KANG Zhi qian, "Research on ESB- based Enterprise Application Integration, " in Second Asia-Pacific Conference on Information Processing, 2010

12.M. P. Papazoglou, Web Services - Principles and Technology. Prentice Hall, 2008.