International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015
ISSN 2091-2730

IMPENDING KNOW-HOW TECHNOLOGY FOR INFORMATION MANAGEMENT WILL BE: OPEN TO CLOUD COMPUTING, IT‟S CRAM AND SAFETY MEASURES

Sonal P. Kothari
K.K.Shah Jarodwala Manigar Science College
Msc.Chemistry Department
Gujarat University
Ahmadabad, India
sonalpkothari@gmail.com

***Abstract*—** Research in virtualization, utility computing, distributed computing, and more recently networking, web and software services has provided chance to build a moderately latest term CLOUD COMPUTING. Cloud Computing implies a service on demand, service oriented architecture, complete information technology transparency for the end-user, vast flexibility, with less total cost of ownership, on-demand services and much more.
The next leading edge in cloud computing security and conformity will be to generate transparency at the bottom-most layers of the cloud by mounting the standards, tools and linkages. If safety of organizations computing infrastructure cannot be trusted, the security of important data, software and services operation on zenith of that infrastructure falls into uncertainty. We believe clouds can extend the organization infrastructure-level policy controls and the security of end-to-end user, to handle even the most demanding safety measures of necessities for data and applications. Finally, this will facilitate organizations to take gain advantage of the cloud's benefits in supporting a vast range of business processes. This paper discusses upcoming technology for information management that is the concept of "cloud" computing, several of security issues it tries to address[1].

Keywords—*"cloud" computing, virtual computing lab, virtualization, utility computing, end-to-end quality of Service.*

I. INTRODUCTION

According to Google Proposal Cloud computing means the endless intelligence of the crowds.
Exact Meaning of Cloud computing:
It is a latest Computing paradigm, that involve computation and data outsourcing, having
(i)On exact "just-in-time" provisioning
(ii) No upfront charge … pay-as-you-go
(iii) Flexible and vast resource scalability

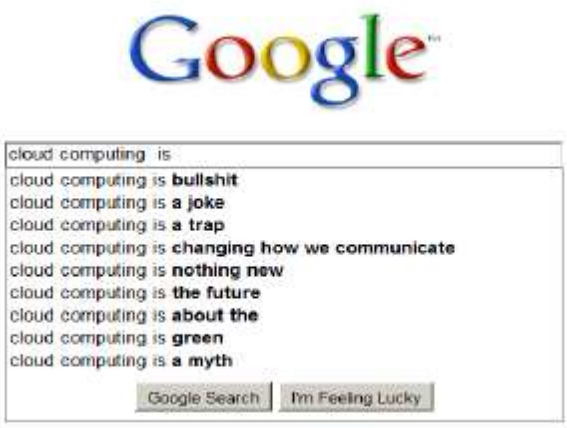

Figure 1.0: Google search image

Cloud Computing is with the aim of, use only when you want, use as much or as less you need, and pay only what you use.
Cloud computing is Internet-based computing, whereby shared servers provide resources, software, and data to computers and other devices on demand, as with the electricity grid. Cloud computing is a natural evolution of the widespread adoption of virtualization, service-oriented architecture and utility computing[1].
Cloud computing means selling "X as a service"
IaaS: Infrastructure as a Service
– Selling virtualized hardware
PaaS: Platform as a service

– Access to a configurable platform/API
SaaS: Software as a service
– Software that runs on top of a cloud

II. CLOUD COMPUTING ARCHITECTURAL LAYERS

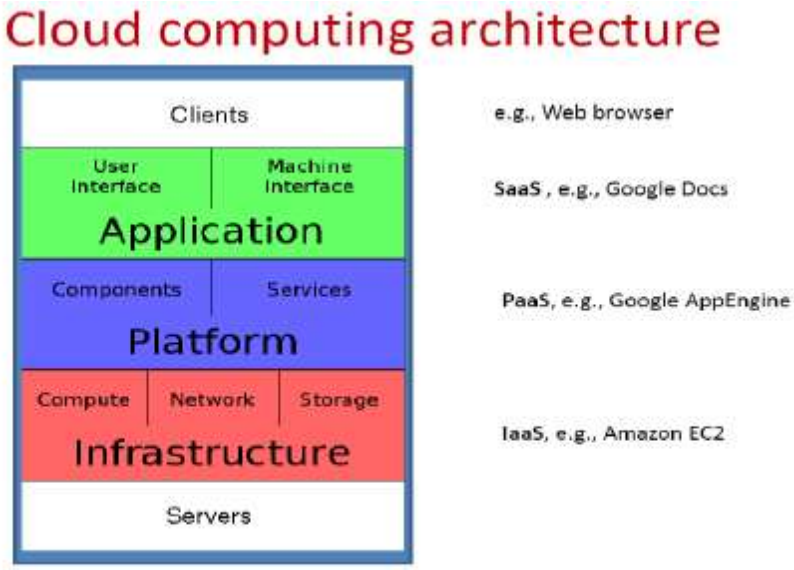

FIGURE 2.1: ARCHITECTURE

FIGURE 2.1: ARCHITECTURE

The Internet functions through a series of network protocols that form a stack of layers, as shown in the figure (or as described in more detail in the OSI model). Once an Internet connection is established among several computers, it is possible to share services within any one of the following layers[2].

Client

A cloud client consists of computer hardware and/or computer software that relies on cloud computing for application delivery, or that is specifically designed for delivery of cloud services and that, in either case, is essentially useless without it. Examples include some computers, phones and other devices, operating systems and browsers.

Application

Cloud application services or "Software as a Service (SaaS)" deliver software as a service over the Internet, eliminating the need to install and run the application on the customer's own computers and simplifying maintenance and support. People tend to use the terms „SaaS" and „cloud" interchangeably, when in fact they are two different things.

Key characteristics include:

• Network-based access to, and management of, commercially available (i.e., not custom) software
• Activities that are managed from central locations rather than at each customer's site, enabling customers to access applications remotely via the Web
• Application delivery that typically is closer to a one-to-many model (single instance, multi-tenant architecture) than to a one-to-one model, including architecture, pricing, partnering, and management characteristics
• Centralized feature updating, which obviates the need for downloadable patches and upgrades.

Platform

Cloud platform services or "Platform as a Service (PaaS)" deliver a computing platform and/or solution stack as a service, often consuming cloud infrastructure and sustaining cloud applications. It facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers.

Infrastructure

Cloud infrastructure services, also known as "Infrastructure as a Service (IaaS)", delivers computer infrastructure - typically a platform virtualization environment - as a service. Rather than purchasing servers, software, data-center space or network equipment, clients instead buy those resources as a fully outsourced service. Suppliers typically bill such services on a utility computing basis and amount of resources consumed (and therefore the cost) will typically reflect the level of activity. IaaS evolved from virtual private server offerings.

Server

The server"s layer consists of computer hardware and/or computer software products that are specifically designed for the delivery of cloud services, including multi-core processors, cloud-specific operating systems and combined offerings.

2.1. Cyber Infrastructure

"Cyber infrastructure makes applications dramatically easier to develop and deploy, thus expanding the feasible scope of applications possible within budget and organizational constraints, and shifting the scientist"s and engineer"s effort away from information technology development and concentrating it on scientific and engineering research. Cyber infrastructure also increases efficiency, quality, and reliability by capturing commonalities among application needs, and facilitates the efficient sharing of equipment and services." Today, almost any business or major activity uses, or relies in some form, on IT and IT services. These services need to be enabling and appliance-like, and there must be an economy of-scale for the total-cost-of-ownership to be better than it would be without cyber infrastructure[3].

Technology needs to improve end-user productivity and reduce technology-driven overhead. For example, unless IT is the primary business of an organization, less than 20% of its efforts not directly connected to its primary business should have to do with IT overhead, even though 80% of its business might be conducted using electronic means.

2.2. Concepts

A powerful underlying and enabling concept is computing through service-oriented architectures

(SOA) – Delivery of an integrated and orchestrated suite of functions to an end-user through composition of both loosely and tightly coupled functions, and services – often network based. Related concepts are component-based system engineering, orchestration of different services through workflows, and virtualization.

2.2.1. Service-oriented Architecture

SOA is not a new concept, although it again has been receiving considerable attention in recent years [9, 25, 38].

Examples of some of the first network-based service-oriented architectures are remote procedure calls (RPC), DCOM and Object Request Brokers (ORBs) based on the CORBA specifications [32, 33]. A more recent example are the so called "Grid Computing" architectures and solutions [15, 17, 18]. In an SOA environment, end-users request an IT service (or an integrated collection of such services) at the desired functional, quality and capacity level, and receive it either at the time requested or at a specified later time. Service discovery, brokering, and reliability are important, and services are usually designed to interoperate, as are the composites made of these services. It is expected that in the next 10 years, service-based solutions will be a major vehicle for delivery of information and other IT-assisted functions at both individual and organizational levels, e.g., software applications, web-based services, personal and business "desktop" computing, high-performance computing[4].

2.2.2. Components

The key to a SOA framework that supports workflows is componentization of its services, an ability to support a range of couplings among workflow building blocks, fault-tolerance in its data- and process-aware service-based delivery, and an ability to audit processes, data and results, i.e., collect and use provenance information. Component-based approach is characterized by [13, 28] reusability (elements can be re-used in other workflows), substitutability (alternative implementations are easy to insert, very precisely specified interfaces are available, runtime component replacement mechanisms exist, there is ability to verify and validate substitutions, etc.), extensibility and scalability (ability to readily extend system component pool and to scale it, increase capabilities of individual components, have an extensible and scalable architecture that can automatically discover new functionalities and resources, etc.), customizability (ability to customize generic features to the needs of a particular scientific domain and problem), and composability (easy construction of more complex functional solutions using basic components, reasoning about such compositions, etc.). There are other characteristics that also are very important. Those include reliability and availability of the components and services, the cost of the services, security, total cost of ownership, economy of scale, and so on. In the context of cloud computing we distinguish many categories of components: from differentiated and undifferentiated hardware, to general purpose and specialized software and applications, to real and virtual "images", to environments, to no-root differentiated resources, to workflow-based environments and collections of services, and so on. They are discussed later in the paper.

2.2.3. Workflows

An integrated view of service-based activities is provided by the concept of a workflow. An ITassisted workflow represents a series of structured activities and computations that arise in information-assisted problem solving. Workflows have been drawing enormous attention in the database and information systems research and development communities [16, 20]. Similarly, the scientific community has developed a number of problem solving environments, most of them as integrated solutions [19]. Scientific workflows merge advances in these two areas to automate support for sophisticated scientific problem solving [28, 42]. A workflow can be represented by a directed graph of data flows that connect loosely and tightly coupled (and often asynchronous) processing components. One such graph is shown in Figure 1. It illustrates a Kepler-based implementation of a part of a fusion simulation workflow [2, 8]. In the context of "cloud computing", the key questions should be whether the underlying infrastructure is supportive of the workflow oriented view of the world. This includes on demand and advance-reservation-based access to individual and aggregated computational and other resources, autonomics, ability to group resources from potentially different "clouds" to deliver workflow results, appropriate level of security and privacy, etc.

2.2.4. Virtualization

Virtualization is another very useful concept. It allows abstraction and isolation of lower level functionalities and underlying hardware. This enables portability of higher level functions and sharing and/or aggregation of the physical resources. The virtualization concept has been around in some form since 1960s (e.g., in IBM mainframe systems). Since then, the concept has matured considerably and it has been applied to all aspects of computing – memory, storage, processors, software, networks, as well as services that IT offers. It is the combination of the growing needs and the recent advances in the IT architectures and solutions that

is now bringing the virtualization to the true commodity level. Virtualization, through its economy of scale, and its ability to offer very advanced and complex IT services at a reasonable cost, is poised to become, along with wireless and highly distributed and pervasive computing devices, such as sensors and personal cell-based access devices, the driving technology behind the next wave in IT growth[5].

III. CLOUD COMPUTING SECURITY ISSUES

Cloud Computing Challenges and Related Security Issues. A Survey Paper identified seven issues that need to be addressed before enterprises consider switching to the cloud computing model. They are as follows:

. Privileged user access - information transmitted from the client through the Internet poses a certain degree of risk, because of issues of data ownership; enterprises should spend time getting to know their providers and their regulations as much as possible before assigning some trivial applications first to test the water

. Regulatory compliance - clients are accountable for the security of their solution, as they can choose between providers that allow to be audited by 3rd party organizations that check levels of security and providers that don't

. Data location - depending on contracts, some clients might never know what country or what jurisdiction their data is located

. Data segregation - encrypted information from multiple companies may be stored on the same hard disk, so a mechanism to separate data should be deployed by the provider.

. Recovery - every provider should have a disaster recovery protocol to protect user data

. Investigative support - if a client suspects faulty activity from the provider, it may not have many legal ways pursue an investigation

. Long-term viability - refers to the ability to retract a contract and all data if the current provider is bought out by another firm

Given that not all of the above need to be improved depending on the application at hand, it is still paramount that consensus is reached on the issues regarding standardization. Third party secure data publication applied to cloud.

Cloud Security and Compliance – What the future holds

The next frontier in cloud security and compliance will be to create transparency at the bottom-most layers of the cloud by developing the standards, tools and linkages to monitor and prove that the cloud‟s physical and virtual machines are actually performing as they should. Verifying what‟s happening at the foundational levels of the cloud is important for the simple reason that if organizations can‟t trust the safety of their computing infrastructure, the security of all the data, software and services running on top of that infrastructure falls into doubt[6].

There‟s currently no easy way for organizations to monitor actual conditions and operating states within the hardware, hypervisors and virtual machines comprising their clouds. However, cloud providers and members of the IT Industry are collaborating on a conceptual IT framework to integrate the secure measurements provided by a hardware root of trust into adjoining hypervisors and virtualization management software. The resulting infrastructure stack would be tied into data analysis tools and a governance, risk & compliance (GRC) console, which would contextualize conditions in the cloud‟s hardware and virtualization layers to present a reliable assessment of an organization‟s overall security and compliance posture. This type of integrated hardware-software framework would make the lowest levels of the cloud‟s infrastructure as inspect able, analyzable and reportable for compliance as the cloud‟s top-most application services layer.

With this unprecedented level of visibility, we believe clouds can develop the infrastructure-level policy controls and the end-to-end security attestations to handle even the most demanding security requirements for applications and data. Ultimately, this will enable organizations to take advantage of the cloud‟s benefits in supporting a much broader range of business processes. Maintaining the Integrity of the Specifications

IV. EXPANSION OF CLOUD COMPUTING OFFERS SECURITY FOR VIRTUALIZATION, CLOUD COMPUTING

Virtualization and cloud computing allow computer users access to powerful computers and software applications hosted by remote groups of servers, but security concerns related to data privacy are limiting public confidence -- and slowing adoption of the new technology. Now researchers from North Carolina State University have developed new techniques and software that may be the key to resolving those security concerns and boosting confidence in the sector.

Virtualization allows the pooling of the computational power and storage of multiple computers, which can then be shared by multiple users. For example, under the cloud computing paradigm, businesses can lease computer resources from a data center to operate Web sites and interact with customers -- without having to pay for the overhead of buying and maintaining their own IT infrastructures. The virtualization manager, commonly referred to as a "hypervisor," is a type of software that creates "virtual machines" that operate in isolation from one another on a common computer. In other words, the hypervisor allows different operating systems to run in isolation from one another -- even though each of these systems is using computing power and storage capability on the same computer. This is the technique that enables concepts like cloud computing to function.

One of the major threats to virtualization -- and cloud computing -- is malicious software that enables computer viruses or other malware that have compromised one customer's system to spread to the underlying hypervisor and, ultimately, to the systems of other customers. In short, a key concern is that one cloud computing customer could download a virus -- such as one that steals user data -- and then spread that virus to the systems of all the other customers.

"If this sort of attack is feasible, it undermines consumer confidence in cloud computing," Jiang says, "since consumers couldn't trust that their information would remain confidential."

But Jiang and his Ph.D. student Zhi Wang have now developed software, called HyperSafe, that leverages existing hardware features to secure hypervisors against such attacks. "We can guarantee the integrity of the underlying hypervisor by protecting it from being compromised by any malware downloaded by an individual user," Jiang says. "By doing so, we can ensure the hypervisor's isolation."
For malware to affect a hypervisor, it typically needs to run its own code in the hypervisor. HyperSafe utilizes two components to prevent that from happening. First, the HyperSafe program "has a technique called non-bypassable memory lockdown, which explicitly and reliably bars the introduction of new code by anyone other than the hypervisor administrator," Jiang says. "This also prevents attempts to modify existing hypervisor code by external users."
Second, HyperSafe uses a technique called restricted pointer indexing. This technique "initially characterizes a hypervisor's normal behavior, and then prevents any deviation from that profile," Jiang says. "Only the hypervisor administrators themselves can introduce changes to the hypervisor code."
The research was funded by the U.S. Army Research Office and the National Science Foundation. The research, "HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor Control-Flow Integrity," will be presented May 18 at the 31st IEEE Symposium On Security And Privacy in Oakland, Calif[7].

V. CONCLUSION

"Cloud" computing builds on decades of research in virtualization, distributed computing, utility computing, and, more recently, networking, web and software services. It implies a service-oriented architecture, reduced information technology overhead for the end-user, great flexibility, reduced total cost of ownership, on demand services and many other things. This paper discusses the concept of "cloud" computing, the issues it tries to address, related research topics, and a "cloud" implementation based on which we can manage information and can make better use of technology.

REFERENCES:

[1] http://www.cloudsecurity.org

[2] M.Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, On Technical Security Issues in Cloud Computing . IEEE, 2009

[3] Rajkumar Buyya, Introduction to the IEEE Transactions on Cloud Computing, Vol-1, January-June 2013.

[4] Rooshabh Kothari, Krishna Kant Lavania, G.L.Saini and Harshraj Yagnik, STEGANOGRAPHY TECHNIQUE BASED MOBILE BANKING SYSTEM, Jounral of

[5] Alistair Croll, "Why Cloud Computing Needs Security", 2008

[6] Jonothan Erickson, "Best Practices for Protecting Data in the Cloud", 2008.
[7] Geva Perry, "How Cloud & Utility Computing Are Different", 2008