Volume : 2 | Issue : 3 | March 2013 • ISSN No 2277 - 8160

Research Paper | Computer Science

Cloud Computing: Security Issues and Challenges

Amit Garg Assistant Professor, IIET, Kinana (Hry.)

Gundeep Tanwar Associate, Professor, BRCMCET, Bahal (Hry.)

ABSTRACT

Cloud computing allows people to share distributed resources and services that belong to various organizations and sites. The service oriented, loose coupling, strong fault tolerant, business model and ease use are main characteristics of cloud computing. However, despite the surge in activity and interest, there are significant, persistent concerns about cloud computing that are impeding momentum and will eventually compromise the vision of cloud computing as a new IT procurement model .In this paper, a proposed method to build a trusted computing environment for cloud computing system by integrating the trusted computing platform into cloud computing system has developed with a vast attention to the security requirements in cloud computing environment

KEYWORDS: Cloud computing,grid computing, service oriented, loose coupling,

1.Cloud Computing

Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flowcharts and diagrams.

A cloud service has three distinct characteristics that differentiate it from traditional hosting. It is sold on demand, typically by the minute or the hour; it is elastic in nature -- a user can have as much or as little of a service as they want at any given time; and the service is fully managed by the provider (the consumer needs nothing but a personal computer and Internet access). Significant innovations in virtualization and distributed computing, as well as improved access to high-speed Internet and a weak economy, have accelerated interest in cloud computing.

A cloud can be private or public. A public cloud sells services to anyone on the Internet. (Currently, Amazon Web Services is the largest public cloud provider.) A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people. When a service provider uses public cloud resources to create their private cloud, the result is called a virtual private cloud. Private or public, the goal of cloud computing is to provide easy, scalable access to computing resources and IT services.

Cloud computing is a term referring to both the platform & the application. It is TCP/IP based integration of computer technologies such as fast micro processor, huge memory, high speed network & reliable system architecture. Cloud computing would have not been possible if standard interconnect protocols & data central technologies are not present. Cloud computing platforms allow dynamic provisions, configuration, deconfiguration & deprovision server as needed. Server in cloud computing can be physical or virtual machine. Advanced cloud includes SAN's firewall & other security devices. It also includes application that is accessible via internet. These cloud applications use large data centers and powerful servers that host Web applications and Web services. Anyone with a suitable Internet connection and a standard browser can access a cloud application. A cloud can batch style back end job & interactive & user friendly applications. It allow workload to be deployed & scaled quickly through virtual or physical machine. It support redundant, self recovering, highly scalable programming models that allow workload to recover from unavoidable hardware & software failures. Cloud computing support grid computing but its not be mixed with Cloud computing. Grid computing involves division of larger tasks into smaller sub tasks that can be run parallel on different servers. Grid requires number of computers, in thousands & commonly used servers, desktops & laptops but cloud computing is not just collection of computer resources as it also provide the mechanism to manage those resources. Cloud also support non grid environment 3-tier web architecture running standard & 2.0 web applications. Management of resources in cloud computing refers to provisioning, change request, reimaging, workload rebalancing, monitoring & deprovisioning.

Beside the web email, the Amazon Elastic Compute Cloud (EC2) [2], Google App Engine [3] and Sales force's CRM [4] largely represent a promising conceptual foundation of cloud services. The services of cloud computing are:-

Characteristics	Cloud Computing	Grid Computing
Commercial Pattern	Yes	Yes
Strong Fault Tolerant	Yes	Half
Loose Coupling	Yes	Half
TCP/IP Based	Yes	Half
Commercial Pattern	Yes	No

Table1.1 Cloud computing Vs. Grid Computing Characteristics

2.Characteristics of Cloud Computing

Table 1.1 depicts the comparison between cloud computing & grid computing. . The "Yes" and "No" stand for cloud computing or grid computing has the special characteristic or not. The "Half" means not owning the whole characteristic & possessing it partially. This paper doesn't focus on comparison between these to rather it focuses on the characteristics or special features of Cloud computing. All Grid, Cloud, HPC(High Performance Computing) & Data centre computing belongs to parallel computing. HPC focuses on scientific computing which is computing intensive and delay sensitive. So high processing performance and low delay are the most important criteria in HPC. Grid computing is based on HPC center. Many connected HPC centers form a large grid which owns a powerful underlying concept – service oriented architectures (SOA).Some creative & impressive concept are yet to be come into reality like utility & autonomic computing. Cloud computing is more accepted than grid computing. Data center which doesn't only pursue powerful processing performance and low delay is more balanced than HPC center.

Service oriented

The concept of service orientation is analogous but more practical then the concept of SOA in Grid computing. Abstraction & Accessibility are two main key features of service oriented conception. Via virtualization & other latest technologies the underlying concept can be extracted without exposing much to user. . Abstraction reduces both the need for cloud user to learn the detail of cloud architecture and the threshold of application development. The key elements of underlying architecture can be accessed easily by user. . Cloud user can consume all the capacity easily by exploring system parameters such as processing performance and

storage capacity. As per the type of capability provided the services of Cloud can be categorized as: Infrastructure-as-a- service (IaaS) , Platform-as-a-service (PaaS) & Software-as-a-service.[5-6].

Infrastructure-as-a-Service is the delivery of huge computing resources such as the capacity of processing, storage and network. For eg. Using storage as a cloud service user has to pay just the consuming part without buying any disk or even knowing nothing about the location of data he deals with. It is sometimes also refer to as Hardware-as-a-service.

Platform-as-a-service generally abstracts the infrastructures and supports a set of application program interface to cloud applications. It generally act as the interface or middle layer between hardware & application. Many big companies want to grasp the chance of predominating the platform of cloud computing as Microsoft does in personal computer time due to the importance of platform in present scenario. The well known examples are Google App Engine [5] and Microsoft's Azure Services Platform [18].

Software-as-a-service aims at replacing the software running on PC. It provide the advantage of allowing us not to buy the software at relatively higher prices but instead using the pay per use pattern thus deteriorating the cost. There is no need to install & run the special software in your PC while using SaaS. The concept of SaaS is attractive and some software runs well as cloud computing, but the delay of network is fatal to real time or half real time applications such as 3D online game.

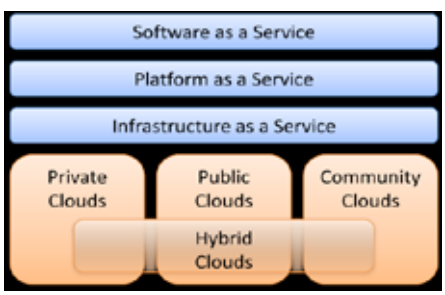


Figure 2.1: Cloud computing deployment and service models

Figure 2.1 provides an overview of the common deployment and service models in cloud computing, where the three service models could be deployed on top of any of the four deployment models

2.2 Storage fault tolerant

Fault can occur at four places in Cloud Computing: provider-inner, provider-across & provider-user.

(1) If a fault occurs in provider, the backup or redundancy of provider will substitute for the failed part. Stop services and restart are another common method if the services are not on time or urgent.
(2) If a fault occurs among providers, the provider-across transaction will be canceled and return with an error hint. Redirecting to other providers is a universal method which involves load balance of whole cloud system. Fortunately, there are only fewer transactions, which are caused by background management in the main, involving more than one provider. It needs only to run background management one time per day or even per week.

Ease Use

Ease use in only simple but also elegant in nature. To evaluate whether the application is successful or not user experience which belong to human computer interaction is one of the main criteria. In cloud computing user interaction results in enhancement or improvement than its ancestors like grid computing. . The cloud service is a means toward the end of providing a good experience for cloud user. The valuable services should be easily accessed by cloud user. The core of user experience is achieving ease use. There are reasons why cloud computing should be ease of use they are as follows:

Firstly most of cloud providers offer internet based interface which is much simpler than API i.e. Application programming Interface. These interfaces are simple and elegant enough to hide the business processing behind. The interfaces can stay the same ignoring whether the business processing has changed or not

Secondly, user experience of web applications is fully studied. So the user interfaces are independent of content. The development of web application has a full suite of flow which can be divided into three stages as mentioned- user need analysis, function design and program implementation. In top-down method, the user experience design is the fundamental of whole function design. The facets of the user experience are useful, usable valuable, desirable, findable, credible and accessible [23].

Cloud Computing Challenges Every new release or discovery has certain challenges so cloud computing; it currently faces following challenges on being deployed in large scale enterprise:

Self-healing:–

In case of application/ network, data storage failure, there will always be a backup running without major delays, making the resource switch appear seamless to the user.

SLA-driven:

Cloud is administrated by service level agreements that allow several instances of one application to be replicated on multiple servers if need arises; dependent on a priority scheme, the cloud may minimize or shut down a lower level application.

Multi-tenancy:-

the cloud permits multiple clients to use the same hardware at the same time, without them knowing it, possibly causing conflicts of interest among customers.

Service-oriented:

Cloud allows one client to use multiple applications in creating its own.

Virtualized:

Applications are not hardware specific; various programs may run on one machine using virtualization or many machines may run one program.

Linearly scalable:

Cloud should handle an increase in data processing linearly; if "n" times more users need a resource, the time to complete the request with "n" more resources should be roughly the same.

Data management:

Distribution, partitioning, security and synchronization of data.

3.Security Challenges

Start-up companies often lack the protection measures to whether off an attack on their servers due to the scarcity of resources - poor programming that explores software vulnerabilities (PHP, JavaScript, etc) open ports to firewalls or inexistent load-balance algorithms susceptible to denial of service attacks. For this reason, new companies are encouraged to pursue cloud computing as the alternative to supporting their own hardware backbone. However cloud computing does not come without its pitfalls.

Data Security

Security is the major concern. Security mainly composes of 3 goals, they are as follows: confidentiality, Integrity & availability.

Confidentiality refers to who stores the encryption keys - data from company A, stored in an encrypted format at company B must be kept secure from employees of B; thus, the client company should own the encryption keys

Integrity refers to the face that no common policies exist for approved data exchanges; the industry has various protocols used to push different software images or jobs. One way to maintain data security on the client side is the use of thin clients that run with as few resources as possible and do not store any user data, so passwords cannot be stolen. The concept seems to be impervi-

ous to attacks based on capturing this data. Integrity means that assets can be modified only by authorized parties only in authorized ways. Integrity comprises of: precise, accurate, meaningful, usable, modifiable by authorized parties only, consistent. Availability means that assets are accessible to authenticated parties at appropriate time whenever the services are required they must be available.

Cloud Computing Security Issues
[Gartner08] seven issues are being recognized for addressing before any enterprise considers switching to the cloud computing model. They are as mentioned:

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 Simply refers to the location the place where your data is present. 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
Recovery here refers to recovery for disastrous or harmful situations or malicious software. 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.

4.Cloud Computing System with Trusted Security
The trusted computing mechanism provides the criteria to provide security measures & a very secure environment. Trusted computing platform is the base for trusted computing, model of trusted computing came into scenario in order to provide privacy & trust in personal platform. Internet computing or network computing is in the scenario from last century, the model of trusted computing is being developed to the network computing, especially distributed system environment. The cloud computing is a promising distributed system model and will act as an important role in the e-business or research environments. Web service technology have developed as quickly and have been used broadly, cloud computing system could evolve to cloud computing service, which integrates the cloud computing with web service technology. So we could extend the trusted computing mechanism to cloud computing service systems by integrating the TCP into cloud computing system.

4.1 Authentication cloud computing environment with TCP
Cloud computing consisting of large number of entities so there is a need for entities to prove their identification to cloud computing system administration. It include entities from users & resources from different sources, therefore authentication is essential at the same time complicated. Considering this we use TCP to aid the process of authentication. TCP is based on TPM. TPM is a logical independent hardware which resist from software as well as hardware attack. The TPM contain a private master key which is capable of providing the protection to other information stored in cloud computing system. Because the hardware certificate can store in TPM, it is hard to attack it. So TPM can provide the trust root for users. AS user have full information of their identity the cloud computing system can use some mechanism to trace the user & determine its origin i.e. point of generation. . Because in the TCP the user's identity is proved by user's personal key and this mechanism is integrated in the hardware, such as the BIOS and TPM, so it is very hard to the user to make deceiving for their identity information. Each site in the cloud computing system will record the visitor's information. So by using the TCP mechanism in cloud computing, the trace of participants can be known by the cloud computing trace mechanism.

4.2 TCP based Data Security in Cloud
With the help of TCP different entities are being enabled to communicate in a secure way. The TCP generate random numbers & then create session key. The random key generated by physical hardware posses better security features than those created by software programs. The Security cloud to call TSS to use the TPM. Then encryption & session key are provided to communicators in cloud computing. With its computing capacity, TPM can burden few computation works from CPU and improve the performance. The important data stored in the computer can be encrypted with keys. While accessing these data firstly the user or the application has to pass the authentication with TPM & then encryption keys are stored with TPM which provide resistance from the attacks. To prevent the attack on integrity of data apply hash function The TPM will check the critical data in a certain interval to protect the integrity of data. The processes of encryption and integrity check use TSS to call the function of TPM.

Tracing of the User's Behavior
As the user is available with the full information of their identity cloud computing system provide the mechanism to trace the user & to determine its origin. in the TCP the user's identity is proved by user's personal key and this mechanism is integrated in the hardware, such as the BIOS and TPM, so it is very hard to the user to make deceiving for their identity information. When the user log in to the cloud computing system the user identification information must be recorded first & verified. Each site in the cloud computing system will record the visitor's information. So if the TCP mechanism is integrated into the cloud computing, the trace of the participants, including the users and other resources, can be knew by the cloud computing trace mechanism. So providing us the mechanism to find out the guilty the one who is performing malicious work & punishing them. In order to provide trusted cloud computing environment the mechanism should not only provide us the information of what the participant/user can do but also enrich us with what the participants/users have done. So monitoring function system must be integrated with cloud computing system in order to enhance the performance i.e. participants behavior. Reference monitor are used in operation system for more than several decades & it will be definitely proved successful in cloud computing too.

5. New Direction for Cloud Users
We now describe some elements of our vision. The core issue is that with the advent of the cloud, the cloud provider also has some control of the cloud users' data. We aim to provide tools supporting the current capabilities of the cloud while limiting cloud provider control of data and enabling all cloud users to benefit from cloud data through enhanced business intelligence.

Information-centric security
Information centric security here refers to protection of data from outside to protection of data from within. In order for enterprises to extend control to data in the cloud, we propose shifting from protecting data from the outside (system and applications which use the data) to protecting data from within. This self protection mechanism requires an intelligence that must be built within the data itself. Data needs to be self-describing and defending, regardless of its environment. Data needs to be encrypted and packaged with a usage policy. When accessed, data should consult its policy and attempt to re-create a secure environment

using virtualization and reveal itself only if the environment is verified as trustworthy (using Trusted Computing). Information-centric security is a natural extension of the trend toward finer, stronger, and more usable data protection.

5.2High-Assurance Remote Server Attestation

We have noted that lack of transparency in data is resulting in moving away of Business from cloud. Data owners wish to audit how their data is being maintained & handled at cloud & in particular the wish to have assurance that their data is secure & not leaked or being abused. or at least have an unalterable audit trail when it does happen. Currently customers must be satisfied with cloud providers using manual auditing procedures like SAS-70.

A promising approach to address this problem is based on Trusted Computing. Imagine a trusted monitor installed at the cloud server that can monitor or audit the operations of the cloud server. The trusted monitor can provide "proofs of compliance" to the data owner, stating that certain access policies have not been violated. To ensure integrity of the monitor, Trusted Computing also allows secure bootstrapping of this monitor to run beside (and securely isolated from) the operating system and applications. The monitor can enforce access control policies and perform monitoring/auditing tasks. To produce a "proof of compliance", the code of the monitor is signed, as well as a "statement of compliance" produced by the monitor. When the data owner receives this proof of compliance, it can verify that the correct monitor code is run, and that the cloud server has complied with access control policies.

5.3Privacy Enhanced Business Intelligence

A different approach (strategy) for retaining control of data is to provide encryption to all cloud data. The problem with encryption is that it limits the use of data especially it result in searching & indexing problem. For eg. It's easy to search the data when it is in clear text but in case of cipher text it is a area of concern. State-of art cryptographers has now result in development of techniques which can solve the above problems. Cryptographers has developed versatile encryption in order to do computation operation & searching on cipher text. For example, searchable encryption allows the data owner to compute a capability from his secret key. A capability to encode a search query, and the cloud can use this capability to decide which documents match the search query, without learning any additional information. Other cryptographic primitives such as homomorphism encryption [20] and Private Information Retrieval (PIR) [12] perform computations on encrypted data without decrypting. As these cryptographic techniques mature, they may open up new possibilities for cloud computing security. In many areas their still lies the probability of being improved so that this cryptographic tools become more practical to cloud. . In particular, even encrypted data can enable anomaly detection that is valuable from a business intelligence standpoint. . For example, a cloud payroll service might provide, with the agreement of participants, aggregate data about payroll execution time that allows users to identify inefficiencies in their own processes. Taking the vision even further, if the cloud service provider is empowered with some ability to search the encrypted data, the proliferation of cloud data can potentially enable better insider threat detection (e.g. by detecting user activities outside of the norm) and better data loss prevention (DLP) (e.g. through detecting anomalous content).

6.Conclusion and Future Work

Cloud computing is the most popular notion in IT today. It is likely to have the same impact on software that foundries have had on the hardware industry. They go on to recommend that "developers would be wise to design their next generation of systems to be deployed into Cloud Computing". While many of the predictions may be cloud hype, we believe the new IT procurement model offered by cloud computing is here to stay. Whether adoption becomes as prevalent and deep as some forecast will depend largely on overcoming fears of the cloud. Cloud fears largely stem from the perceived loss of control of sensitive data. Current control measures do not adequately address cloud computing third-party data storage and processing needs. In our vision, we propose to extend control measures from the enterprise into the cloud through the use of Trusted Computing and applied cryptographic techniques. These measures should alleviate much of today's fear of cloud computing, and, we believe, have the potential to provide demonstrable business intelligence advantages to cloud participation.

This paper discusses the characteristics and concept of trusted security in cloud computing. The conception service oriented characteristic abstracts the details of cloud computing implementation. The loose coupling and strong fault tolerant stand for the main technical characteristics. Owning the business model is the key differentiation compared with other academic researches and helps cloud computing flourishing. The ease use user experience characteristics helps cloud computing being widely accepted by non computer experts. We believe that these characteristics expose the essential of cloud computing and the development and adoption of this evolving technology will benefit from our work. The analyzed trusted computing in the cloud computing environment and the function of trusted computing platform in cloud computing. The advantages of proposed approach are to extend the trusted computing technology into the cloud computing environment to achieve the trusted computing requirements for the cloud computing and then fulfill the trusted cloud computing. TCP is used as the hardware base for the cloud computing system. In this design, TCP provides cloud computing system some important security functions, such authentication, communication security and data protection. The TCP provides cloud computing a secure base for achieve trusted computing.

REFERENCES

[1] IBM, "Google and IBM Announced University Initiative to Address Internet-Scale Computing Challenges,"http://www-3.ibm.com/press/us/en/pressrelease/22414.wss [2] Amazon, "Amazon Web Services," http://aws.amazon.com/. [3] Google, "Google app Engine," http://code.google.com/appengine/. Salesforce, "CRM", http://www.salesforce.com/. [4] [searchcloudcomputing.com,"What is cloud computing?" http://searchcloudcomputing.techtarget.com/sDefinition/0,,sid201_gci1287881,00.html. [5] L.M. Vaquero, L.R. Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, v.39 n.1, 2009. [6] Wikipedia, "Cloud computing," http://en.wikipedia.org/wiki/Cloud_computing. [7] J. Geelan, "Twenty one experts define cloud computing. Virtualization," Electronic Magazine, http://virtualization.sys [8] D. Farber, "Oracle's Ellison nails cloud computing," http://news.cnet.com/ 8301-13953_3-10052188-80.html. [9] [R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," [10] P. Sharma, "What kind of apps are best suited for 'Cloud deployment' : 4 Solutions," [11] http://www.techpluto.com/cloud- computing characteristics/. [12] International Journal on Cloud Computing: Services and Architecture(IJCCSA),Vol.1, No.3, November 2011 [13] D. Amrhein, "Forget Defining Cloud Computing," http://ibm.ulitzer.com/ node/1018801. [14] Microsoft,"WindowsAzure," http://www.microsoft.com/windowsazure/ windows azure/. [15] P. Watson, P. Lord, F. Gibson, P. Periorellis, and G. Pitsilis, "Cloud computing for e-science withCarmen," IBERGRID, 2008, pp.1-5, [16] Erickson08] Jonothan Erickson, "Best Practices for Protecting Data in the Cloud", 2008 [17] http://www.ddj.com/security/210602698 [18] [Brodkin08] Jon Brodkin, "Seven Cloud-Computing [OCC08] The Open Cloud Consortium, 2008 http://www.opencloudconsortium.org/index.html [19] Gu08] Yunhong Gu, Robert L. Grossman: Sector and Sphere: The Design and Implementation of a High Performance Data Cloud, UK, 2008. [20] [Reese09] George Reese, "Cloud Application Architectures", April 2009, O'Reilly Media.