International Journal of Pure and Applied Mathematics
Volume 116 No. 10 2017, 27-32
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

DISTRIBUTED COMPUTING: SECURITY ISSUES AND CHALLENGES

A V ALLIN GEO[1], Dr.K.P.Kaliyamurthie[2]
`[1]Assistant Professor[2]Dean, Dept. of CSE,
BIST,BIHER, BharathUniversity ,
Chennai, Tamil Nadu, India
[1]seemeallin@gmail.com, [2]kpkaliyamurthie@gmail.com

Abstract: Distributed computing is a structure for providing figuring supplier by means of the web on request and pay in venture with utilize get right of section to a pool of shared assets particularly organizes, capacity, servers, offerings and bundles without substantial gaining them. So it spares taking care of cost and time for organizations. Numerous ventures, such as keeping money, social insurance ,tutoring and programming businesses like Accenture are likewise moving towards the cloud in light of the effectiveness of administrations gave by method for the compensation in venture with-utilize design in view of the sources, for example, handling vitality utilized, exchanges finished, transmission capacity expended, information exchanged, or carport range possessed et cetera. Distributed computing is an exceptionally web based innovation wherein client realities is spared and keep up inside the data focal point of a cloud guarantor like Google, Amazon, Salesforce.com and Microsoft and so on.

Keywords: Cloud models, cloud security issues, cloud security, cloud architecture, Data protection.

1. Introduction

Cloud Computing is a allotted structure that centralizes server assets on a scalable platform in an effort to provide on call for computing assets and offerings. Cloud carrier companies (CSP's) provide cloud systems for his or her clients to use and create their web services, much like net carrier carriers provide costumers high velocity broadband to access the net. CSPs and ISPs (Internet Service Providers) both provide offerings. Cloud computing is a version that permits convenient, on-call for network get right of entry to a shared pool of configurable computing resources which include networks, servers, garage, programs that can be unexpectedly provisioned and launched with minimal management effort or provider provider's interplay. In widespread cloud vendors offer three kinds of services I.E. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). There are diverse motives for organizations to move closer to IT answers that encompass cloud computing as they are simply required to pay for the assets on intake foundation. In addition, companies can without problems meet the desires of rapidly changing markets to make sure that they're continually at the leading edge for their clients [1,2]

- The transmission of personal sensitive records to the cloud server
- The transmission of facts from the cloud server to clients' computers
- The storage of clients' personal facts in cloud servers which might be faraway server not owned via the clients.[3]

2. Cloud computing building blocks

Different models of cloud computing: Generally cloud services may be divided into three categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

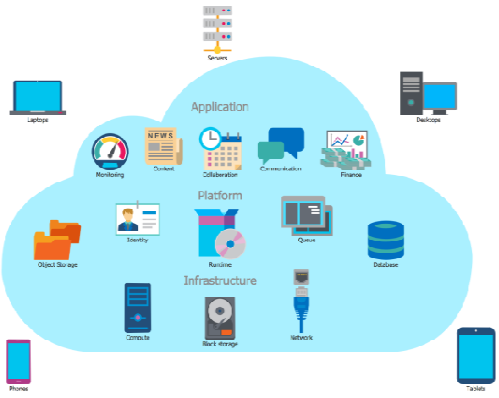

Figure 1. cloud bilding blocks architecture

Software-as-a-Service (SaaS)

SaaS may be defined as a method by which Application Service Provider (ASP) provide specific software program programs over the Internet. This makes the patron to dispose of installing and operating the application on personal pc and also eliminates the super load of software program maintenance; continuing operation, safeguarding and guide SaaS supplier advertently takes duty for deploying and coping with the IT infrastructure (servers, working system software,

databases, records centre area, network get admission to, energy and cooling, and many others) and processes (infrastructure patches/enhancements, utility patches/enhancements, backups, and many others.) required to run and manage the whole solution. SaaS capabilities a whole utility offered as a provider on demand. Examples of SaaS consist of: Salesforce.Com, Google Apps[8,9].

Platform as a Service (PaaS)

"PaaS is the transport of a computing platform and solution stack as a provider without software downloads or set up for developers, IT managers or quit-customers. It offers an infrastructure with a excessive stage of integration that allows you to put into effect and test cloud programs. The consumer does now not control the infrastructure (which includes network, servers, working structures and storage), however he controls deployed packages and, probable, their configurations. Examples of PaaS consist of: Force.Com, Google App Engine and Microsoft Azure[10,11].

Infrastructure as a Service (IaaS)

Infrastructure as a carrier (IaaS) refers to the sharing of hardware sources for executing services using Virtualization technology. Its most important goal is to make resources which include servers, network and storage extra effortlessly handy by using applications and working systems. Thus, it gives basic infrastructure on-call for services and the use of Application Programming Interface (API) for interactions with hosts, switches, and routers,

And the functionality of including new equipment in a simple and obvious manner. In trendy, the person does no longer control the underlying hardware inside the cloud infrastructure, but he controls the working systems, garage and deployed programs. The provider issuer owns the equipment and is answerable for housing, running and preserving it. The client generally can pay on a in keeping with-use foundation. Examples of IaaS consist of Amazon Elastic Cloud Computing (EC2), Amazon S3, and Go Grid. There are also four unique cloud deployment models specifically Private cloud, Public cloud, Hybrid cloud and Community cloud.[12,13]

Private cloud

Private cloud can be owned or leased and managed via the organization or a 3rd celebration and exist at on premises or off-premises. It is greater pricey and comfy while in comparison to public cloud. In private cloud there aren't any additional safety policies, criminal requirements or bandwidth limitations that can be present in a public cloud environment, via using a personal cloud, the cloud provider providers and the customers have optimized manipulate of the infrastructure and advanced protection, given that consumer's get admission to and the networks used are restrained. One of the high-quality examples of a non-public cloud is Eucalyptus Systems[14].

Public Cloud

A cloud infrastructure is furnished to many customers and is managed by using a third celebration and exists beyond the business enterprise firewall. Multiple businesses can work at the infrastructure supplied, at the equal time and customers can dynamically provision resources. These clouds are fully hosted and controlled by the Cloud Company and absolutely obligations of set up, management, provisioning, and preservation. Customers are best charged for the resources they use, so beneath-usage is removed. Since customers have little control over the infrastructure, methods requiring effective protection and regulatory compliance are not continually a very good suit for public clouds. In this model, no get admission to regulations may be implemented and no authorization and authentication techniques may be used. Public cloud companies along with Google or Amazon offer an access manage to their customers. Examples of a public cloud include Microsoft Azure, Google App Engine. [15]

Hybrid Cloud

A composition of or greater cloud deployment models, related in a manner that statistics switch takes area among them without affecting every other. These clouds could generally be created through the employer and management obligations could be cut up among the agency and the cloud issuer. In this version, a corporation can outline the goals and desires of offerings. A nicely-constructed hybrid cloud can be useful for providing relaxed services inclusive of receiving client payments, in addition to those that are secondary to the business, consisting of employee payroll processing.

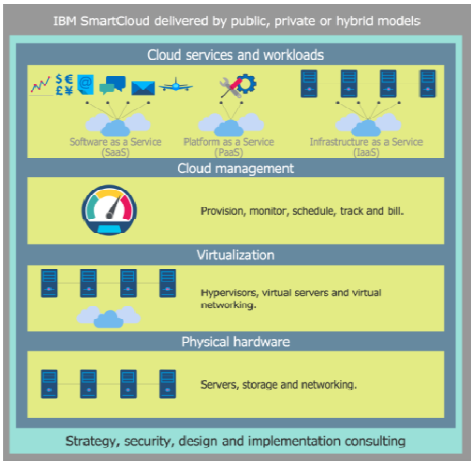

Figure 2. cloud services and work load

Community Cloud

Infrastructure shared by means of numerous companies for a shared motive and can be managed by using them or a third birthday celebration service company and rarely provided cloud model. These clouds are commonly primarily based on an settlement among associated commercial enterprise companies consisting of banking or academic businesses. A cloud surroundings working in keeping with this model may exist regionally or remotely. An instance of a Community Cloud consists of Face book[18,19]

Cloud computing security architecture

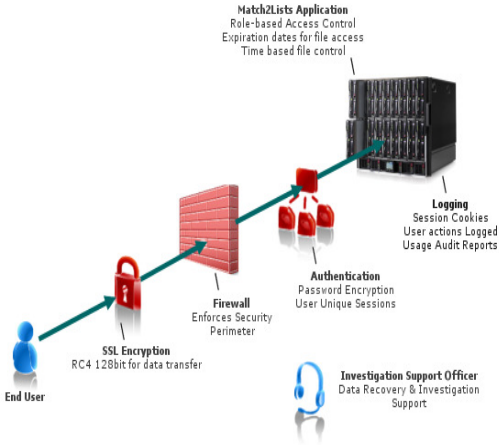

Figure 3. cloud security architecture

There are several protection troubles for cloud computing as it encompasses many technology inclusive of networks, databases, working structures, virtualization, resource scheduling, transaction control, load balancing, concurrency control and memory management. Therefore, security troubles for lots of those structures and technology are applicable to cloud computing. For instance, the community that interconnects the systems in a cloud needs to be comfortable. Furthermore, virtualization paradigm in cloud computing results in several safety concerns. For instance, mapping the digital machines to the bodily machines must be finished securely.

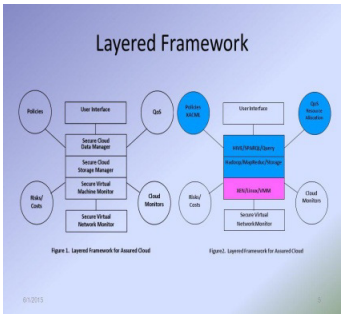

Figure 4. cloud Layered Framework

Cross reducing services are furnished through the coverage layer, the cloud tracking layer, the reliability layer and the chance analysis layer. For the Secure Virtual Machine (VM) Monitor we're combining both hardware and software program answers in digital machines to address problems inclusive of key logger analyzing XEN developed at the University of Cambridge and exploring protection to fulfil the needs of our applications (e.g., relaxed dispensed storage and information management). For Secure Cloud Storage Management, we're developing a garage infrastructure which integrates assets from a couple of providers to shape a massive virtual storage system

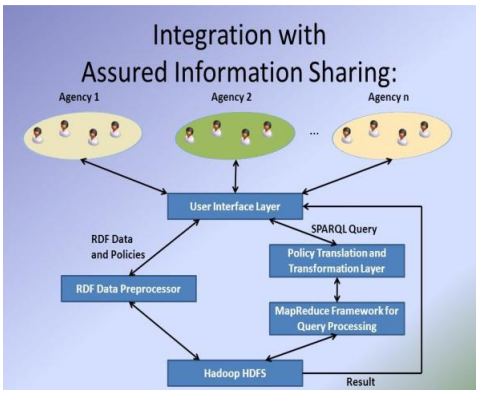

Figure 5. Cloud Assured Information Sharing

Illustrates the technology we're using for every of the layers. This assignment is being performed in close collaboration with the AFOSR MURI venture on Assured Information Sharing and EOARD funded studies undertaking on coverage control for facts sharing. We have completed a robust demonstration of at ease query processing. We have also developed secure storage algorithms and completed the design of XACML for Hadoop.

Key security issue in cloud computing

Cloud computing consists of programs, structures and infrastructure segments. Each phase plays specific operations and gives different merchandise for agencies and people around the sector. The business application consists of Software as a Service (SaaS), Utility Computing, Web Services, Platform as a Service (PaaS), Managed Service Providers (MSP), Service Commerce and Internet Integration. Access to server & Application

- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability
- Data Segregation
- Security Policy and Compliance
- Patch management[5]

Access to Servers & Applications:

In conventional data centers, administrative get entry to servers is managed and restricted to direct or on-premise connections which are not the case of cloud facts facilities. In cloud computing administrative access must be conducted thru the Internet, growing publicity and risk. It is extremely crucial to restriction administrative get entry to to statistics and screens this access to keep visibility of modifications in gadget control. Data get admission to issue is especially associated with security policies supplied to the customers even as getting access to the records. In a typical situation, a small commercial enterprise enterprise can use a cloud supplied by using a few other provider for wearing out its commercial enterprise methods. A specific set of facts.

Data Transmission

Encryption techniques are used for statistics in transmission. To offer the protection for records best is going in which the client wishes it to head by the usage of authentication and integrity and isn't changed in transmission. SSL/TLS protocols are used right here. In Cloud environment most of the information is not encrypted inside the processing time. But to manner facts, for any application that fact ought to be unencrypted. In a totally homomorphism encryption scheme enhance in cryptography, which lets in statistics to be processed without being decrypted. To provide the confidentiality and integrity of information-in-transmission to and from Cloud Company by using the use of get entry to controls like authorization, authentication, auditing for the use of assets, and make sure the supply of the Internet-dealing with sources at cloud issuer. Man-in-the-middle attacks is cryptographic attack is achieved when an attacker can area themselves inside the communication direction among the customers. Here, there's the opportunity that they can interrupt and change communications.

Virtual mach insecurity:

Virtualization is one of the important components of a cloud. Virtual machines are dynamic i.e. it can speedy be reverted to previous instances, paused and restarted, exceedingly easily. Ensuring that unique instances running at the same physical device are remote from each other is a main task of virtualization. They also can be readily cloned and seamlessly moved between bodily servers. This dynamic nature and capability for VM sprawl makes it hard to gain and keep steady safety. Vulnerabilities or configuration errors may be unknowingly propagated. Also, it's far tough to keep an auditable document of the safety state of a digital machine at any given point in time. Full Virtualization and Para Virtualization are styles of virtualization in a cloud computing paradigm. In complete virtualization, whole hardware architecture is replicated surely.

Network Security

Networks are categorised into many types like shared and non-shared, public or non-public, small area or huge location networks and every of them have a number of protection threats to address. Problems related to the network stage protection comprise of DNS attacks, Sniffer assaults, issue of reused IP.

Data protection

For fashionable consumer, its miles pretty clean to discover the possible garage at the aspect that offers the provider of cloud computing. To attain the provider of cloud computing, the maximum not unusual applied verbal exchange protocol is Hypertext Transfer Protocol (HTTP). In order to guarantee the facts protection and facts integrity, Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) are the most commonplace adoption. In a conventional on-premise utility deployment version, the touchy statistics of every organisation maintains to are living inside the business enterprise boundary and is concern to its physical, logical and employees protection and access manipulate regulations. However, in cloud computing, the corporation records is stored outdoor the agency boundaries, at the Service issuer end. Consequently, the provider issuer should adopt additional safety assessments to make sure information protection and prevent breaches due to safety vulnerabilities inside the utility or thru malicious employees. This entails using robust encryption strategies for facts protection and pleasant-grained authorization to govern access to data. Cloud service companies which include Amazon, the Elastic Compute Cloud (EC2) directors do now not have get admission to patron instances and cannot log into the Guest OS.

Data Privacy

The facts privateness is also one of the key concerns for Cloud computing. A privateness steering committee need to additionally be created to assist make selections related to statistics privacy. Requirement: This will make sure that your organisation is prepared to fulfil the statistics privacy demands of its customers and regulators. Data in the cloud is commonly globally allotted which raises concerns approximately jurisdiction, facts publicity and privateness. Organizations stand a risk of not complying with government rules as would be explained further while the cloud vendors who reveal touchy facts hazard felony liability. Virtual co-tenancy of sensitive and non-touchy information at the identical host additionally consists of its very own capability risks.

Challenges of cloud computing

Cloud computing research addresses the demanding situations of meeting the necessities of next generation personal, public and hybrid

Cloud computing architectures, additionally the demanding situations of allowing applications and development systems to take advantage of the benefits of cloud computing. The studies on cloud computing remains at an early degree. Many current troubles have no longer been completely addressed, while new demanding situations hold emerging from industry programs. Some of the hard studies troubles in cloud computing are given below[4].

- Service Level Agreements (SLA's)
- Cloud Data Management & Security
- Data Encryption
- Migration of virtual Machines
- Interoperability
- Access Controls
- Energy Management
- Multitenancy
- Server Consolidation
- Reliability & Availability of Service
- Common Cloud Standards
- Platform Management [2]

3. Conclusion and feautre work:

One of the largest protection worries with the cloud computing version is the sharing of assets. Cloud carrier providers want to inform their customers on the level of security that they offer on their cloud. In this paper, we first discussed diverse fashions of cloud computing, protection troubles and research challenges in cloud computing. Data protection is fundamental problem for Cloud Computing. There are numerous different safety demanding situations which includes safety factors of community and virtualization. This paper has highlighted these kind of issues of cloud computing. We agree with that because of the complexity of the cloud, it'll be difficult to obtain end-to-end protection. New security strategies want to be developed and older safety techniques needed to be radically tweaked so that you can paintings with the clouds structure. As the improvement of cloud computing era is still at an early degree, we hope our paintings will provide a higher know-how of the design demanding situations of cloud computing, and pave the way for similarly studies on this region[3].

References

[1] Kevin Hamlen and Murat Kantarcioglu, The University of Texas at Dallas, USA
international Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010
[2] Rabi Prasad Padhy, ManasRanjanPatra and Suresh Chandra Satapathy (IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS)in 2011
[3] Monjur Ahmed and Mohammad Ashraf Hossain2 (1) senior Lecturer, Daffodil Institute of IT, Dhaka, Bangladesh. (2)Freelance IT Consultant, Dhaka, Bangladesh.(International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014)
[4] Kevin hamlen, Murat kantarcioglu and BhavaniThurisingham university of Texas at Dallas U.S.A
[5] Latifur Khan, The University of Texas at Dallas, USA BhavaniThuraisingham, The University of Texas at Dallas, USA.
[6] Udayakumar R., Kaliyamurthie K.P., Khanaa, Thooyamani K.P., Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, v-29, i-14, pp-86-90, 2014.