American Journal of Applied Sciences 11 (8): 1224-1228, 2014
ISSN: 1546-9239
© 2014 Chakravarthy and Kannan, This open access article is distributed under a Creative Commons Attribution (CC-BY) 3.0 license
doi:10.3844/ajassp.2014.1224.1228 Published Online 11 (8) 2014 (http://www.thescipub.com/ajas.toc)

A REVIEW ON SECURED CLOUD COMPUTING ENVIRONMENT

Hemanth Chakravarthy, M. and E. Kannan

Department of Computer Science and Engg, Veltech Technical University, Chennai, India

Received 2014-03-30; Revised 2014-04-15; Accepted 2014-05-06

ABSTRACT

Nowadays, the scientific problem becomes very complex; therefore, it requires more computing power and storage space. These requirements are very common in an organization while dealing with current technological data and requirements. Based on these basic requirements, need of higher computational resources is an important issue when dealing with current technological methodology. Hence, cloud computing has become the most important computing paradigm of recent world. The cloud computing is an open source and using Internet as network model. Rapid growth in the field of "cloud computing" also increases severe security concerns, because security has a constant issue. This study reviews security models of cloud computing.

Keywords: Cloud Computing, Security, High Performance Computing, Framework

1. INTRODUCTION

Cloud computing is a kind of high performance computing (HPC). HPC includes distributed computing, grid computing and cloud computing. The past technologies such as distributed computing and parallel computing are not highly suitable for the recent advancements because, the modern computer industry is operating very large amounts of data which is geographically, distributed. Distributed computing is a paradigm which focuses on wide range of users with a distributed access to scalable, virtualized hardware and software infrastructure.

Grid computing is a paradigm of resource sharing which offers wide and collective distributed computing. The emergence of cloud computing from distributed and grid computing will provide promise to save money by making it imperative for organizations. Software as a Service (SaaS) is a cloud service which focus on providing users with business-specific capabilities such as email, or customers management, for example, Google Apps, Sales force.com and Zoho.com. Infrastructure as a Service (IaaS) is another type of cloud capability which provides mainly for on demand computational infrastructure available over the internet, such as storage space. Some of the IaaS are, Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Solution (S3), Go-Grid, IBM Computing on Demand (COD), Microsoft live mesh and Rack space cloud.

The third cloud computing capability is termed as Platform as a Service (PaaS), in which application development platform are rented as a resource to the users to leverage the resources of established organizations. Some of the PaaS are, Akamai Edge platform, Force.com, Google App Engine, Microsoft Azure service platform and Yahoo! open Strategy (Y!oS) (Chandramohan and Baskaran, 2010; 2011).

The basic attributes of cloud computing are listed below:

- Availability-Users have the ability to access their resources at any time through a standard internet connection
- Collaboration-Users begin to see the cloud as a way to work simultaneously on common data and information

Corresponding Author: Hemanth Chakravarthy, M., Department of Computer Science and Engg, Veltech Technical University, Chennai, India

- Elasticity-Provides transparently manages a user's resources utilization based on dynamically changing needs
- Lower infrastructure-The pay per usage model allows an organization to only pay for resources they need with a basically no investment in the physical resources available in cloud
- Mobility-Users have the ability to access data and applications from the globe
- Risk Reduction-Organizations can use the cloud to test ideas and concepts before making investments in technology
- Scalability-Users have access to a larger amount of resources their scale based on their demand
- Virtualization-Each user's has a single view of the available resources, independently of how they are arranged in terms of physical device
- Computational risk to implement cloud computing-Some key organizational concerns can act as barriers to the adoption of cloud computing. This concerns are interoperability, latency, platform or language constraints, regulations, reliability, resource control and security

This study further reviews recent research in cloud computing in the past few years

2. MATERIALS AND METHODS

2.1. Review on HPC

Abrishami *et al*. (2012) analysed the processing speed, computational power and other resources in distributed and parallel computing environments. So, in the past few years, the grid computing has been proposed as an effective resource management in order to meet the organizational requirements.

Mateescu *et al*. (2011) proposed HPC architecture for grid and cloud computing environments. They considered the predictable execution of scientific applications and scales from a single resource to multiple resources, with different ownership, policy and geographic locations for architectural design patterns. They identified three paradigms namely, (1) owner-centric HPC (traditional), (2) grid computing and (3) cloud computing. They studied three architectures which include grid, cloud and HPC. Their nature in terms of capacity, capability, resource sharing is shown in **Table 1**. This HPC architecture is applicable where the grid and cloud computing system is integrated.

Today's hybrid computing ecosystem, given by Keqin (2005), represents the intersection of three broad paradigms for computing infrastructure and use:

- Owner-centric (traditional) HPC
- Grid computing (resource sharing)
- Cloud computing (on-demand resource/service provisioning)

Each paradigm is characterized by a set of attributes of the resources, making up the infrastructure and executing the applications on that infrastructure. These attributes include:

- Resource ownership: Either locally owned resources or externally owned resources
- Resource accessibility: Either private (only by the owner of the resource) or public (available to entities other than the owner)
- Resource sizing: Either quasi-static (resources grow when purchasing new hardware) or dynamic (resources can grow dynamically by using external, public, resources)
- Resource allocation policy: Either exclusive (per-organization, or per-group, or per-project, or per-user) or shared among organizations, groups, projects, or users
- Application portability: Either tied to a specific platform (e.g., hardware, operating system) or platform-agnostic (easily portable)

In terms of these attributes, the following three paradigms combine to support hybrid computing. In Owner-centric HPC, presented by Singh *et al*. (2008), resources are locally owned, with private access (for members of the owner organization and its partners); resources have quasi-static size that changes by purchasing new resources. In cloud computing, resources can be either externally owned (public cloud), or internally owned (private cloud), the former being offered by cloud providers. Public clouds offer access to external users who are typically billed on a pay-as-you-use basis.

QoS-oriented is also an important aspect in cloud computing. The availability of cloud computing resources is analysed from QoS of a single cloud resource node. Dong *et al*. (2013) proposed QoS Oriented monitoring model, in which, a monitoring model of cloud computing, dynamic process of the cloud computing service, described by common attribution and special attribution to QoS of some cloud resources.

Table 1. Comparison of grid, cloud and HPC

Attribute	HPC	Grid	Cloud
Capacity	Fixed	Average to high; growth by aggregating independently manged resources	High; growth by elasticity of commonly mamged resources
Capability	Very high	Average to high	Low to average
Virtual machine support	Rarely	Sometimes	Always
Resource sharing	Limited	High	Limited
Resource heterogeneity	Low	Average to high	Low to average
Built-in workload management	Yes	Yes	No
Distribute workload across resources from multiple admin domains	Not applicable	Yes	No
Interoperability	Not applicable	Average	Low
Security	High	Average	Low to average

2.2. Review on Cloud Computing

For the past few years, the cloud computing is one among top 10 growing technology, which proves a significant impact on IT in the future. However, there are lacks of security models, frameworks and certificates in cloud computing. ISO 27000 and NIST-FISMA provides cloud certificate in the recent days. These cloud security certificates help cloud providers to improve the consumers trust. Even though, these standards are still lacking from covering the full complexity of the cloud computing model.

Zhang and Zhang (2009) analyzed the security issues in the cloud computing, briefed about the Open Cloud Computing Federation (OCCF). Zhang and Zhang (2009) proposed Mobile Agent Based Open Cloud Computing Federation (MABOCCF) mechanism. MABOCCF combines the mobile agent and cloud computing to provide a realization for the open cloud computing federation. MABOCCF offrs multiple heterogeneous cloud computing platforms and realizes portability and interoperability.

Defining a framework is an initial process of the security model of cloud computing. A cloud security management framework is proposed by Almorsy *et al*. (2011). This framework is based on aligning the FISMA standard to fit with the cloud computing model. This framework is based on improving collaboration between cloud providers and service providers, which defined on top of a number of security standards.

2.3. Review on Security in Cloud Computing

In the world of cloud computing, there are lacks of compliance to standards, reporting, monitoring, service level agreements and legal acts. The providers have data-centers worldwide and customer can dynamically allocate their data among various data centers. Hence, this creates the customers anxiety because they may not know where their data is at any given time. Service providers and most governments have the ability to track and manage records. Most of these data will flow in and out of their environments. Here the major concern is the level of trust and transparency of the customer which should be well known to the customers through proper documents and policies, also the customers can test and identify their trust level at any point of time.

The biggest benefit of cloud computing is the centralization of data. Organizations have an issue with asset protection, in no small part because of data being stored in numerous places, like laptops and the desktop. Thick clients are apt to download files and maintain them on the hard drive and there are plenty of laptops out there with non-encrypted files. Using thin clients creates a better chance for centralized data storage. As such, there's less chance for data leakage. Centralization also provides the opportunity for better monitoring. That data is in one place makes it easier to check in on user data and verify that access.

The same security issues that the organization deals with are the sorts of issues that SaaS providers will faces the securing network, hardware issues, applications and data. But compliance adds another level of headache. Regulations like Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLBA) and industry standards like the Payment Card Industry Data Security Standard (PCI DSS) make things particularly challenging. Prior to SaaS, compliance could be managed by a few tasks:

- Identify users and access privileges
- Identify sensitive data
- Identify where it's located
- Identify how it is encrypted
- Document this for auditors and regulators

The security aspects in cloud computing is listed in detail below:

- Application security
- Business continuity and disaster
- Data governance
- Data privacy
- Data security
- Education and training
- Forensics
- Identity Access Management (IAM)
- Investigations
- Logging for compliance and security
- Password assurance testing
- Physical security
- Policies, standards and guidelines
- Recovery
- Risk assessment
- Risk management
- Secure software development
- Security architecture design
- Security awareness
- Security governance
- Security images
- Security management
- Security monitoring and incident
- Security portfolio management
- Third-party risk management
- Virtual machine security
- Vulnerability assessment

The development of secured cloud involves identifying specific threats and the risks they represent, followed by design and implementation of specific controls to counter those threats and assist in managing the risks they pose to the organization and/or its customers. This must provide consistency, repeatability and conformance. The SDLC of secured cloud consists of six phases, which are:

- Phase 1. Investigation:-Define project processes and goals and document them in the program security policy
- Phase 2. Analysis:-Analyze existing security policies and programs, analyze current threats and controls, examine legal issues and perform risk analysis
- Phase 3. Logical design:-Develop a security blueprint, plan incident response actions, plan business responses to disaster and determine the feasibility of continuing and/or outsourcing the project
- Phase 4. Physical design:-Select technologies to support the security blueprint, develop a definition of a successful solution, design physical security measures to support technological solutions and review and approve plans
- Phase 5. Implementation:-Buy or develop security solutions. At the end of this phase, present a tested package to management for approval
- Phase 6. Maintenance:-Constantly monitor, test, modify, update and repair to respond to changing threats

Public-key encryption schemes are secure only if the authenticity of the public key is assured. A public-key certificate scheme provides the necessary security (Stallings, 2005). A simple public-key algorithm is Diffie-Hellman key exchange. This protocol enables two users to establish a secret key using a public-key scheme based on discrete logarithms. The protocol is secure only if the authenticity of the two participants can be established.

3. RESULTS

Implementation of cloud become more rapid in the recent years, such as Wu and Huang (2011), Mehdi *et al*. (2011), Kumar and Balasubramanie (2012) and Ponnuramu and Tamilselvan (2012). Wu and Huang (2011) implemented quasi-experimental method was applied to the study of 110 fifth grade students of Tunglo Elementary School, Taiwan. Mehdi *et al*. (2011) proposes Impatient Task Mapping in Elastic Cloud using Genetic Algorithm. This algorithm finds a fast mapping using genetic algorithms. The genetic algorithm with “exist if satisfy” condition is speeding up the mapping process. The genetic algorithm is implemented using Cloudsim.

Infrastructure as a Service (IaaS) is one among the cloud services that provides a computing resourses for demand in various applications like Parallel Data processing. The computer resources offered in the cloud are extremely dynamic and probably heterogeneous. Nephele is the data processing framework used to exploit the dynamic resource allocation offered by IaaS clouds for task scheduling.

4. DISCUSSION

The quasi-experiment results showed that cloud computing was better than traditional IT system of educational environment. Cloudsim simulator is a cloud benchmark which is used to test algorithms in

cloud computing. Mapping time and makespan are the performance metrics in the cloud based mapping algorithms. Tasks scheduling and processing in cloud offers automatically instantiated and terminated job execution. The present methodologies increases the efficacy of the scheduling algorithm for the real time Cloud Computing services. These Algorithms utilizes the Turnaround time which also assigns high priority for task of early completion and less priority for abortions /deadlines issues of real time tasks.

5. CONCLUSION

Wu and Huang (2011) recommended the cloud computing infrastructure to education in real world. The results of genetic algorithm in the cloud environment shows an improvement than MCT algorithm which also improves the throughput, hence can be used to map more jobs to cloud resources. The scheduling algorithms in cloud implemented on both preemptive and Non-premptive methods. It outperfoms than the existing utility based scheduling algorithms on preemptive and Non-preemptive scheduling methods. Hence, a novel Turnaround time utility scheduling approach with high priority and low priority tasks.

The experimental results of secured system shows better results, however there are still critical and performance improvement need to be achieved.

6. REFERENCES

Abrishami, S., M. Naghibzadeh and D. Epema, 2012. Cost-driven scheduling of grid workflows using partial critical paths. IEEE Trans. Parallel Distributed Syst., 23: 1400-1414.

Almorsy, M., J. Grundy and A.S. Ibrahim, 2011. Collaboration-based cloud computing security management framework. Proceedings of the IEEE International Conference on Cloud Computing, (CCC' 11), pp: 364-371.

Chandramohan, B, abd R. Baskran, 2011. Reliable Barrier-Free Services (RBS) for heterogeneous next generation network. Commun. Comput. Inform. Sci., 148: 79-82. DOI: 10.1007/978-3-642-20499-9_13

Chandramohan, B. and R. Baskaran, 2010. Improving network performance using ACO based redundant link avoidance algorithm. Int. J. Comput. Sci.

Dong, W.E., W. Nan and L. Xu, 2013. QoS-oriented monitoring model of cloud computing resources availability. Proceedings of the 5th International Conference on Computational and Information Sciences, (CIS' 13), pp:1537-1540.

Keqin, L., 2005. Job scheduling and processor allocation for grid computing on metacomputers. J. Parallel Distributed Comput., 65: 1406-1418.

Kumar, S.K.S. and P. Balasubramanie, 2012. Dynamic scheduling for cloud reliability using transportation problem. J. Comput. Sci., 8: 1615-1626. DOI: 10.3844/jcssp.2012.1615.1626

Mateescu, G., W. Gentzsch and C.J. Ribbens, 2011. Hybrid computing-where HPC meets grid and cloud computing. Future Generat. Comput. Syst., 27: 440-453.

Mehdi, N.A., A. Mamat, H. Ibrahim and S.K. Subramaniam, 2011. Impatient task mapping in elastic cloud using genetic algorithm. J. Comput. Sci., 7: 877-883. DOI: 10.3844/jcssp.2011.877.883

Ponnuramu, V. and L. Tamilselvan, 2012. Data integrity proof and secure computation in cloud computing. J. Comput. Sci., 8: 1987-1995. DOI: 10.3844/jcssp.2012.1987.1995

Singh, S., Y.K. Loke, and C.D. Furberg, 2008. Inhaled anticholinergics and risk of major adverse cardiovascular events in patients with chronic obstructive pulmonary disease: A systematic review and meta-analysis. JAMA, 300: 1439-1450. DOI: 10.1001/jama.300.12.1439

Stallings, W., 2005. Cryptography and Network Security Principles and Practices. 4th Edn., Prentice Hall.

Wu, C.F. and L.P. Huang, 2011. Developing the environment of information technology education using cloud computing infrastructure. Am. J. Applied Sci., 8: 864-871. DOI: 10.3844/ajassp.2011.864.871

Zhang, Z. and X. Zhang, 2009. Realization of open cloud computing federation based on mobile agent. Proceedings of the IEEE International Conference on Intelligent Computing and Intelligent Systems, pp: 642- 646.