Security and QoS Guarantee-based Resource Allocation within Cloud Computing Environment

Abstract

- Data and services in a Cloud Computing are not limited to a single organization's perimeter and span multiple trusted or untrusted domains.
- In addition, data security and privacy are the most challenging barriers to generalized cloud adoption. In this paper, we propose two architectures (inter-cloud Broker and Federation) enabling best cloud resources selection based on optimal cost, Quality of Service (QoS) and security guarantee for Network as a Service (NaaS) and Infrastructure as a Service (IaaS) services in a Cloud Computing environment.
- We simulate our proposed framework to evaluate the best cloud resources selection and the impact of security on QoS guarantee. The obtained results show this impact and that the Broker architecture is the most economical while ensuring QoS and security requirements

Existing system

- Many organizations, especially small and medium-sized enterprises (SMEs), are adopting this technology to achieve high performance and scalability for their applications while maintaining a rapid access to cloud services with lower Capital Expenditure.
- In addition, a Cloud Service User (CSU) that can be an end-user, a Software as a Service (SaaS) provider, or a Platform as a Service (PaaS) provider, requires for its services an end-to-end Quality of Service (QoS) assurance

Disadvantages

- This renders the service selection process prone to adopting non-optimum provider paths for delivering the composite service, which in many cases does not comply with the required performance and pricing specifications.
- This is an important challenge that will be more and more obliging with the widespread adoption of cloud computing, which necessitates the presence of an autonomic service selection.

Proposed system

- we propose two architectures (inter-cloud Broker and Federation) enabling best cloud resources selection based on optimal cost, Quality of Service (QoS) and security guarantee for Network as a Service (NaaS) and Infrastructure as a Service (IaaS) services in a Cloud Computing environment.
- We simulate our proposed framework to evaluate the best cloud resources selection and the impact of security on QoS guarantee. The obtained results show this impact and that the Broker architecture is the most economical while ensuring QoS and security requirements.

Advantages

- security assurance could have a great impact on the QoS guarantee. In fact, storing and retrieving security information as well as the encryption and decryption of data lead to an increase in network traffic, additional processing consumption and more delay and latency.
- relation between QoS and security, and both need to be carefully managed in a global framework and not separately

Hardware Requirements

- Processor :Intel Pentium IV 1GHz
- RAM :256MB (Min)
- Hard Drive :5GB free space
- Monitor :1024 * 768, High Color inch
- Mouse :Scroll Mouse(Logitech)
- Keyboard :104 keys

Software requirements

- OS : Windows XP/7/8
- Front End : Visual Studio 2010/ netbeans 7.1
- Back End : SQL Server 2005/ heidisql 3.2
- Browser : Any Web Browser

conclusion

- In this paper, we presented two architectures for the best cloud resources selection based on optimal cost and QoS as well as security guarantee for NaaS and IaaS services in conformance with an SLA in a cloud computing environment.
- In addition, we focused on the impact of security assurance on QoS guarantee. Finally, we have evaluated our proposed framework for a cloud videoconferencing application.
- We have obtained good results by enabling good performances for this application. In particular, we have observed that the Broker architecture is the most economical while ensuring QoS and security requirements, in addition to the security impact on QoS guarantee.

References

[1] J. Heiser, M. Nicolett, Assessing the security risks of cloud computing, Gartner, 2008.

[2] W. Itani, C. Ghali, R. Bassil, A. Kayssi, A. Chehab, ServBGP: BGPinspired autonomic service routing for multi-provider collaborative architectures in the cloud, Future Generation Computer Systems, Vol. 32, pp. 99-117, 2014.

[3] Kaspersky, Global Corporate IT Security Risks: 2013, Technical report, pp. 1-26, 2013.

[4] L. Karadsheh, Applying security policies and service level agreement to IaaS service model to enhance security and transition, computers & security, Vol. 31, Iss. 3, pp. 315-326, 2012.

[5] C. Christmann, J. Falkner, A. Horch, H. Kett, Identification of IT Security and legal requirements regarding Cloud services, Sixth International Conference on Cloud Computing, GRIDs, and Virtualization, CLOUD COMPUTING 2015, pp. 1-7, 2015.