Abstract

Cloud Computing is the rising generation key platform for sharing the resources like software as a service, infrastructure as a service, and platform as a service. In future all IT enterprises migrate into cloud platform. Cloud server exchanges the messages for remote location users with the help of multi cloud architectures. Security issues are generated in data transmission. Day by day new vulnerabilities are discovered in cloud computing. Previous cloud development provides the security in limited dimensions with the help of application logic. It not sufficient for control the all different attackers. This is not efficient and scalable environment. It's not optimal approach [1]. Increase the range of cloud computing security and detect the attacks in deep degree manner. It provides highly safe results with good data protection. Here we concentrate on two dimensions. Those dimensions are application logic view and regulatory framework. Its have excellent security properties. This approach provides the excellent security compare to previous approaches. We proved different properties like good integrity and confidentiality compare to previous approaches [1][2].
Enhanced Secured Multi cloud using Technical Environment and Regulatory Framework

References

- Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Ryusuke Masuoka, Jesus Molina, Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control, 2009
- Jeff Naruchitparames and Mehmet Hadi Güunes, Enhancing Data Privacy and Integrity in the Cloud, 2011
- R. Thandeeswaran1, S. Subhashini1, N. Jeyanthi1, M. A. Saleem Durai, Secured Multi-Cloud Virtual Infrastructure with Improved Performance, 2012
- Michael Smit, Mark Shtern, Bradley Simmons, and Marin Litoiu, Enabling an Enhanced Data-as-a-Service Ecosystem, 2011

Index Terms

Computer Science

Security

Keywords

Cloud Computing Multi cloud architectures Security constraints Data Protection model