Abstract

In recent years, cloud computing has been applied increasingly and most of the companies, have considered some kinds of cloud strategies to use in their organizations. Growing request for services causes overload on a single cloud. Cloud federation is an ideal solution to overcome continuous increasing requests by users. Identity management and access control are from challenging subjects of cloud federation which for has been offered approaches like identity federation, although it is not an optimum approach. There is needed a more effective, accurate and safe approach. This paper offered an approach to access control based on risk and trust parameters, depending on learning automata in cloud federation. Results of simulation shows that proposed approach prevents access of unauthorized user to the resources of federation by decreasing primary trust for novice user also by increasing risk for high sensitive resources.


- Abdul Raouf Khan, "Access control in cloud computing environment", Department of Computer Sciences, King Faisal University, Saudi Arabia, MAY 2012.


- Daniel Ricardo dos Santos, Carla Merkle Westphall, "Risk-based dynamic access control for a highly scalable cloud federation", Carlos Becker Westphall Networks and Management Laboratory Federal University of Santa Catarina Florianópolis, Brazil, 2013, 40-63.


- Q. Ni, E. Bertino, J. Lobo, "Risk-based access control systems built on fuzzy inferences", in: Proceedings of the 5th ACM Symposium on Information, Computer and

- Kevin Kelly, "Role-Based Access Control Model", 1998, pp. 50-93.
- Riaz Ahmed Shaikh, Kamel Adi, Luigi Logrippo, "Dynamic risk-based decision methods for access control systems", Université du Qu´ebec en Outaouais, Gatineau, Qu´ebec, Canada, 2011.

Index Terms

Computer Science Distributed Systems

Keywords

Cloud Computation Access Control Cloud Federation Learning Automata.