Abstract

Role-based access control (RBAC) models have generated a great interest in the security community as a powerful and generalized approach to security management and ability to model organizational structure and their capability to reduce administrative expenses. In this paper, we highlight the drawbacks of RBAC models in terms of access control and authorization and later provide a more viable extended-RBAC model, which enhances and extends its powers to make any Cloud Server more secure by adding valuable constraints. Later the Blobs are stored on cloud server which is then accessed by the end users via this Extended RBAC model. We describe a practical implementation of the proposed extended RBAC based architecture and discuss the performance results with its base models. We later show how the users with different premiums can access this architecture in a better way and also how the unknown users for this architecture can be denied the usage of services by adding valuable constraints.

References

- I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing and grid computing 360-degree compared," Grid Computing Environments Workshop, 2008. GCE'08,
Securing Data Storage by Extending Role-based Access Control

2009, pp. 1-10.


Index Terms

Computer Science

Distributed Systems

Keywords

Authorization  RBAC  Blobs  Server  Architecture