A dynamic risk-based access control architecture for cloud computing

Cloud computing is a distributed computing model that still faces problems. New ideas emerge to take advantage of its features and among the research challenges found in the cloud, we can highlight Identity and Access Management. The main problems of the application of access control in the cloud are the necessary flexibility and scalability to support a large number of users and resources in a dynamic and heterogeneous environment, with collaboration and information sharing needs. This paper proposes the use of risk-based dynamic access control for cloud computing. The proposal is presented as an access control model based on an extension of the XACML standard with three new components: the Risk Engine, the Risk Quantification Web Services and the Risk Policies. The risk policies present a method to describe risk metrics and their quantification, using local or remote functions. The risk policies allow users and cloud service providers to define how to handle risk-based access control for their resources, using different quantification and aggregation methods. The model reaches the access decision based on a combination of XACML decisions and risk analysis. A prototype of the model is implemented, showing it has enough expressivity to describe the models of related work. In the experimental results, the prototype takes between 2 and 6 milliseconds to reach access decisions using a risk policy. A discussion on the security aspects of the model is also presented.

Published in: Network Operations and Management Symposium (NOMS), 2014 IEEE

Abstract

Cloud computing is a distributed computing model that still faces problems. New ideas emerge to take advantage of its features and among the research challenges found in the cloud, we can highlight Identity and Access Management. The main problems of the application of access control in the cloud are the necessary flexibility and scalability to support a large number of users and resources in a dynamic and heterogeneous environment, with collaboration and information sharing needs. This paper proposes the use of risk-based dynamic access control for cloud computing. The proposal is presented as an access control model based on an extension of the XACML standard with three new components: the Risk Engine, the Risk Quantification Web Services and the Risk Policies. The risk policies present a method to describe risk metrics and their quantification, using local or remote functions. The risk policies allow users and cloud service providers to define how to handle risk-based access control for their resources, using different quantification and aggregation methods. The model reaches the access decision based on a combination of XACML decisions and risk analysis. A prototype of the model is implemented, showing it has enough expressivity to describe the models of related work. In the experimental results, the prototype takes between 2 and 6 milliseconds to reach access decisions using a risk policy. A discussion on the security aspects of the model is also presented.