Example of data access control models research paper

Technology, Internet

Access control models

Access control models are the mechanisms that are used to regulate the access of users to a computer system or information systems. This paper will discuss three access models and discuss the environments in which they best operate in.

The first access model is the role based access control (RBAC). This access control model does not have a specific environment in which it operates. This is to say that it can be implemented in an operating system, application level or network level, or in database level. The privileges that are users have on the network depend on the role that the users play in the organization. The best environment in which the RBAC model works is the network environment. In a network environment, the values of users which are up-to-date must be made available to all servers in the network. If the attributes of a user are kept on a single server, it will mean that server will have to be accessed across the network. This is because another server on the network might require that user attribute. If the user attributes are kept in each server, then each of these attributes will have to be changed if there are changes which are made to the user attributes.

Another access model is the mandatory access control (MAC) model. This model has its origin in the military where an administrator controls what happens in the network. In this system, the privileges are controlled by the administrator. The control is mandatory. This access control is used in an operating system and a database. The best environment that this is used is the database environment. This is because the users are controlled. There are some database objects and commands that are not to be used by non-administrators. The administrators will therefore identify these objects and set privileges about who will use and who are not allowed to use. This access method will help to control the integrity of the data.

The third access control method is discretionary access control method. In this model, the user sets the privileges that other people will have access on according to their discretion. This model works best in operating system environments. This is because users are allowed to create profiles in the operating systems. With these profiles, users are able to share or restrict some objects they own. They will do this at their own discretion.

References

Angelro, D. (2005). Access control models: Authorization mechanisms for database management systems. Rochester: Rochester Institute of Technology.

Benantar, M. (2006). Access control systems: Security, identity management and trust models . New York: Springer.

Bertino, E., Ghinita, G., & Kamra, A. (2011). Access control for databases: Concepts and systems. Washington: Now Publishers Inc.

Chang, S., University, W. S., & Nio, D. (2008). Access control models for XML data and provenance metadata in scientific workflows. New York: ProQuest.

Garcia-Alfaro, J. (2010). Data privacy management and autonomous spontaneous security. New York: Springer.

Popek, G. J. (2003). Access control models. Boston: Harvard University Press.