Analysis of access control model for data security and privacy on multi-tenant SaaS

ABSTRACT

Cloud computing has become most trending and emerging technology in recent years and has changed the way of computation and services delivered to customer. Despite all the advantages that cloud provides, users still feel insecure to adopt cloud computing and having major concern over the data security and privacy. This is due to the data of numerous tenants are being located in the same location or database. In this environment data access by unauthorized user is possible. To overcome this issue, there should be a clear boundary for each tenant. Access control model is used to grant the right level of permission to the user in order to carry out their duties, to prevent unauthorized access and to protect assets of organizations and systems. Access control model also can prevent unauthorized user from accessing protected data, ensure authorized users can access protected data and prevent authorized users from performing illegal actions on protected data. There are many types of access control model available in the industry. However, not all the models can be applied in cloud environment due to various reasons. This paper presents an analysis of existing role based access control models. We use evaluation criteria that outlined by NIST for access control system. First, we identified a list of criteria that are suitable to apply in cloud environment specifically on data security and privacy of multi-tenant SaaS application in public cloud. Then, we analysed the existing access control models against the identified evaluation criteria. The analysis outlines the important gaps and missing elements of an access control model that can be extended into an access control model based testing.

Keyword: Cloud computing; Data security and privacy; NIST's evaluation criteria; Role based access control model