

## **Role performance trust-based access control for protecting sensitive attributes**

### **ABSTRACT**

Preserving privacy is a challenge and requires the management of access control, which may be based on role, purpose or trust. There are many recent advances of access control models have been developed to avoid unauthorized users access to the privacy. However, there are still issues that impede the development of effective access control. The issue highlight in this paper is inappropriate access and use of sensitive attributes by authorized users. Therefore, it is critical to design an efficient access control model based on trust to protect sensitive attributes from untrusted user. In this paper, we propose a new access control model based on trust called role performance trust-based access control to permit trusted user access to sensitive attributes. Subsequently, we also propose a comprehensive policy to permit user access sensitive attributes based on two trust metrics namely user experience and behaviour. To evaluate the trustworthiness of authorized user, we propose a quantification method to measure those metrics. Based on the results, role performance trust-based access control may significantly permit or prohibit access to personal information, especially sensitive attributes by authorized users. This model is capable to solve the issue of authorized user without trust to access sensitive attributes.

**Keyword:** Privacy protection; Role performance; Sensitive attributes; Trust; Trust based access control