Performance and divisional trust and purpose-based access control for privacy preservation

ABSTRACT

Privacy has been recognized to be a critical requirement in computing environments. To keep the privacy safe from inappropriate use, one of the most popular methods that can be used is the access control. Currently, many augmentation of access control models has been developed to improve the effectiveness in preserving the privacy. However, there are still issues that need improvements. In current Purpose-Based Access Control (PBAC) Models, all authorized users in the domain are allowed to access the personal information especially sensitive attributes equally. It may cause the risk of privacy disclosure by 'limited-authorized' user, i.e., legitimate user but untrusted and unauthorized to access certain personal information with sensitive attributes. In this study a finer-grained access control called performance and divisional trust and purpose-based access control is proposed to prevent limited-authorized user access to the privacy. Based on organizational structure (functional departmentalization) current PBAC Models permit authorized user in the functional level to access the personal information. This model can be set at the next level after the functional level, i.e., the divisional level to access it. Subsequently, a comprehensive policy is proposed to permit user to access sensitive attributes based on two trust metrics namely user experience and behaviour. To evaluate the trustworthiness of the authorized user, a quantification method is proposed to measure those metrics. Based on the results, this model may significantly permit or prohibit access to personal information or with sensitive attributes. Besides, the issue of privacy disclosure by limited-authorized user to access certain privacy is resolved.

Keyword: Access control; Divisional; Purpose; Purpose-based access control; Role performance; Sensitive attributes; Trust