

## **128. CONTEXT RELATED POLICIES ON DATA ISOLATION FOR ORGANIZATIONAL DATA USING PROFILES**

VIGNESH.M, Ms.AISHWARYA.K

M.E Student, Computer Science

Arulmigu Meenakshi Amman College of Engineering, vadamavandal-604410

Kancheepuram, Tamilnadu, India

vig91090@gmail.com, aishumecse@gmail.com

General studies have shown that allowing access to enterprise services with smartphones increases employee productivity. Despite this positive scenario, users can install third-party applications on their smartphones, which may provide some malicious applications to access their company confidential information. This poses serious security concerns to sensitive corporate data. One possible solution to this problem is isolation, by keeping applications and data related to work separated from recreational applications. MOSES a solution for separating modes of use in smartphones. MOSES implements soft virtualization through controlled software. Profiles can be easily and dynamically specified by end users. MOSES provides a GUI for this purpose. Profiles can be fine-grained to the level of single object (e.g., file, SMS) and single application. Isolation Using MOSES creating profiles for securing confidential data but that the applications that have root access to the system can bypass MOSES protection. A Novel Attribute Based Access Control Enabled MOSES method proposed to overcome the problem of these root application bypassing the security profile protections.

Keywords: MOSES, ABAC, GUI, SP, BYOD, Context.

*Journal of Science and Innovative Engineering & Technology*