

Chapter 25

Context–Aware Privacy and Sharing Control in Collaborative Mobile Applications

Ahmad Kamran Malik

Vienna University of Technology, Austria

Atif Manzoor

Vienna University of Technology, Austria

Schahram Dustdar

Vienna University of Technology, Austria

ABSTRACT

Mobile applications are being used in every field of life. Latest advances in mobile computing technology and applications make it a new level of communication proxy for its users. Despite their power as personalized service provider and an internet connected computing device, mobile systems have their inherent limitations, like small display area and limited power and memory, which must be handled in mobile-based applications. Context-awareness is being used to cope with the limitations of mobile systems and is an important area of recent research on mobile and ubiquitous system. Context plays a fundamental role in awareness applications. Activities of mobile users can be monitored by the context provided through sensors connected with user and her environment. One of the basic requirements in context-aware mobile applications is privacy and sharing control in Collaborative Working Environment (CWE). Sharing control, in the authors' system, is the distributed and dynamic control of sharing policies and information being shared. Dynamic nature of context is helpful in making automated decisions based on the current situation, for example, dynamic adaptation of level of context information being shared among collaborating users, dynamic adaptation of sharing control decisions, and dynamic adaptation of rules for sharing control.

DOI: 10.4018/978-1-61520-655-1.ch025

1. INTRODUCTION

In past, privacy and access control policies related to users were centrally administered by enterprise. These policies were usually static in nature, without using context. In current mobile-based dynamic environments, centralized systems and access control policies are being replaced with distributed, peer to peer and, Web-based sharing control policies where users control sharing of their own data. Recent research efforts are focusing on owner-defined context-based dynamic policies for sharing control (Malik et al., 2009). There is a need to shift control of sharing policies from central administrators to owner of context. In this way, distributed and fine-grained level of sharing can be achieved. For dynamic collaborative systems, we motivate use of the term “*sharing control*” in contrast to access control, whose meanings are twofold: owner-based control of context data being shared and sharing of control policies between owner and her enterprise. In untrusted systems, owner of context wants full control of her policies and context. An owner may want to change her policies with change in context and user interaction. Apart from fully restricting user access, different users can be granted different level of access rights based on their role in enterprise and current context. In addition, resource constrained mobile devices also need content adaptation. Both of these scenarios require that context information should be organized in a way so that only certain level of data can be shared whenever needed. In mobile applications, content being sent should be based on context of receiver and receiving device. Only required level of content is sent so that low memory device can store them with less battery consumption and can be easily displayed on small screen (Dorn et al., 2007). Our research efforts include owner-based dynamic sharing control using context of all involved entities, and control of context being shared at fine-grained level of all involved entities. An owner can modify her sharing policy for

any entity, for example, user, activity, team, and enterprise. Context is organized in hierarchical order and sharing control system provides context at a level that is allowed to requesting user. In the following sections, we describe research efforts in areas related to privacy, access control, mobile-based systems, context-based systems, semantic techniques, and Web services, and compare them with our sharing control techniques in CWE. At the end, we describe our architectural framework for owner-based dynamic sharing control.

Section 2 describes collaborative working environments in context of mobile applications. Section 3 explains the privacy, sharing control systems including Role-Based Access control (RBAC) and trust-based systems. In Section 4, context related issues like context-based access control and adaptation techniques for mobile and ubiquitous systems are described. Section 5 describes semantic techniques commonly used for context-based privacy and access control. Importance of Web services and SOA-based systems in mobile computing environment is described in Section 6. We discuss our research work about dynamic sharing control (DySCon) in CWE (Malik et al., 2009), in Section 7. Finally, Section 8 concludes the chapter and describes future work.

2. MOBILE-BASED COLLABORATIVE WORKING ENVIRONMENTS

Collaborative working environment (CWE) is one of the most demanding areas for mobile applications where distributed users having mobile devices collaborate to achieve a common goal. With the advancement of distributed systems and pervasive computing devices, new opportunities and challenges arise in the area of context-based collaborative systems development. Context sharing in dynamic CWE is important for knowing the current state of collaborative tasks. Mobile applications are being used in CWE which may

13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/context-aware-privacy-sharing-control/66481

Related Content

A Proficient Approach for Load Balancing in Cloud Computing-Join Minimum Loaded Queue: Join Minimum Loaded Queue

Minakshi Sharma, Rajneesh Kumarand Anurag Jain (2020). *International Journal of Information System Modeling and Design* (pp. 12-36).

www.irma-international.org/article/a-proficient-approach-for-load-balancing-in-cloud-computing-join-minimum-loaded-queue/250311

Secure by Design: Developing Secure Software Systems from the Ground Up

Haralambos Mouratidisand Miao Kang (2013). *Developing and Evaluating Security-Aware Software Systems* (pp. 1-19).

www.irma-international.org/chapter/secure-design-developing-secure-software/72195

The Role of Programming Models on Reconfigurable Computing Fabrics

Joao M.P. Cardoso, Joao Bispoand Adriano K. Sanches (2010). *Behavioral Modeling for Embedded Systems and Technologies: Applications for Design and Implementation* (pp. 290-316).

www.irma-international.org/chapter/role-programming-models-reconfigurable-computing/36347

Building Secure Software Using XP

Walid Al-Ahmad (2013). *Developing and Evaluating Security-Aware Software Systems* (pp. 161-175).

www.irma-international.org/chapter/building-secure-software-using/72204

Proposals of a Method Detecting Learners' Difficult Points in Object Modeling Exercises and a Tool to Support the Method

Takafumi Tanaka, Kazuki Mori, Hiroaki Hashiura, Atsuo Hazeyamaand Seiichi Komiya (2015). *International Journal of Software Innovation* (pp. 63-74).

www.irma-international.org/article/proposals-of-a-method-detecting-learners-difficult-points-in-object-modeling-exercises-and-a-tool-to-support-the-method/121548