Context and Trust Based Adaptive Security for Accessing Services in Ubiquitous Computing Environment

G. Jagadamba, Department of Information Science and Engineering, Siddaganga Institute of Technology, Tumakuru, India
B Sathish Babu, Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumakuru, India

ABSTRACT

The smart spaces built on the ubiquitous network make the services available for every entity in a seamless way using the most suitable resource provider. However, all services are not equally sensitive; hence do not require the same levels of security. In this paper, the authors propose an adaptive security scheme which handles service requests originating from heterogeneous contexts and belonging to different trust levels. The adaptive security scheme includes user classification, situational analysis and dynamic generation of appropriate security policies. The proposed security scheme can be made use to secure application built on the Ubiquitous Computing Environment (UCE) such as health care, smart office, smart ubiquitous home, etc.

KEYWORDS


1. INTRODUCTION

A ubiquitous computing system is a communication framework which integrates various components such as computing devices, service providers, etc., in the Ubiquitous Computing Environment (UCE) (Grilo, n. d.). The mobility and invisibility of information exchange have resulted in many security and privacy concerns in UCE. Thus, in the new era of ubiquitous computing, a large-scale computing application depends on the assurance of essential security and privacy properties for both service requesters and service providers (Giang, Hung, Lee et al., 2007).

At the side of service provider’s, the provider’s merely tries to provide services to the legitimate service requesters with the proper authentication and authorization process. But, instead of the traditional authentication and authorization techniques operate with the static security methodologies. The static characteristics are not sensitive to the operating device and context. However, the possible solution would be adaptive security scheme built on the ubiquitous network.

The adaptive security in a smart space can monitor user behaviors and give additional permissions to well-behaving users by identifying a suitable authorization level (Ovaska & Evesti, 2011). Hence, the nature of adaptivity involved self-modification on the required security level by adjusting

DOI: 10.4018/IJSSOE.2016100101

Copyright © 2016, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
internal operating parameters (encryption schemes, security protocols, security policies, algorithms, authentication and authorization mechanisms and Quality of Service) by making dynamic changes in the structure of the security system (Savola, Abie & Sihvonen, 2012) for the individual entity. Thus, novel security scheme is proposed that can support a service requester activity in a context and trust centric service access model in the smart spaces. The adaptivity in the security is achieved through the situation analysis (SA), and generation of an applicable and accurate security policy.

The overview of the paper is outlined as literature survey in second section, introduction to the definitions in third section, proposed adaptive security scheme in section 4, results and discussions in section 5, and conclusion with future applications in last section.

2. LITERATURE REVIEW

A service access based on the user behavior (Yarmand, Sartipi & Down, 2013) provided the concept of analyzing the user characteristics while designing an adaptive security policy. Our earlier work (Jagadamba and Sathish Babu, 2016a; Jagadamba & Sathish Babu, 2013) was able to examine the user request through the contextual information before fulfilling the request. The work was more of role and context based service access but did not consider the verification of the truthfulness of the user’s request. However, the basic service access model lacks provisions for context, trust and privacy issues when operated in the distributed environments. An effort to integrate trust and privacy was done in an extended Attribute-Based Access Control model for critical situations for registered and non-registered users (Sun, Lili, Yong et al., 2014). The model facilitates the development of an access policy through the set of access control rules by combining subjects and objects through context and trust parameters. The concept of relating the subject and object to trust is a good idea to design security policies while accessing the services in smart spaces like health care monitoring environment, smart offices, smart campus and so on.

Application based adaptive security from trust level (Bakar, Azmi & Haron, 2014) offered the predefined score cards from the user profile, and context defines the access levels dynamically. The dynamic changes were found in typical scenarios but not in unexpected scenarios like emergency or disaster situations. Adaptations to unexpected situations were attempted (Al Kukhun & Sedes, 2008) for flexible authorization and access to provide balanced service solutions. In an emergency/spontaneous coalition situation, access control for unauthorized users was based on policies by dynamic evaluation and adaptation (Mohan & Blough, 2010). However, the proposal considered predefined policies for emergencies. The policies are acted when emergency locations are identified with the user. In this scheme, the user has defined the emergency context rather than system identifying the emergency content. However, the context centric access control policy enforcement was adopted to make the security system more adaptive in the spontaneous coalition’s situations (Toninelli, Montanari, Kagal, 2006) but, the work was more or less on resource sharing concept in co-located location.

The absence of trusted entity raised a risk in the resource sharing for an unknown entity. Hence, identification of trust is made by an entity while allowing the service access. In the earlier work (Aditya and Sathish Babu, 2012) the adaptive trust was proposed by forming the virtual territory/smart spaces with similar capacity and trust. The model was comparably good with the efficiency (Sabater & Sierra, 2001; Hoque, Rahman & Ahamed, 2009), as the security level was made adaptive using trust attributes. But, in (Leister, Poslad, Hamdi et al., 2014) dynamic policies are generated based on subject, object, purpose and trust attributes in the emergency situations.

The access policies were built (Venkatasubramanian, Mukherjee & Gupta, 2014) according to the situations in the noncritical scenarios rather than critical scenarios. Here, the context determined the purpose of the requester rather than the truthfulness of the user. But, the service provider or organizations can lay the policies according to the degree of service severity. Hence, the policies based on direct and indirect consequences that result due to misappropriation of communications were observed (Sathish Babu & Venkataram, 2009). Finally, from (Jagadamba & Sathish Babu, 2016b) a
Lessons from Practices and Standards in Safety-Critical and Regulated Sectors

Case Study: Version Control in Component-Based Systems
www.igi-global.com/chapter/case-study-version-control-component/74886?camid=4v1a

Threat Representation Methods for Composite Service Process Models
www.igi-global.com/article/threat-representation-methods-composite-service/77914?camid=4v1a