ABSTRACT

The appearance of dynamic distributed networks in early eighties of the last century has evoked technologies like pervasive systems, ubiquitous computing, ambient intelligence, and more recently, Internet of Things (IoT) to be developed. Moreover, sensing capabilities embedded in computing devices offer users the ability to share, retrieve, and update resources on anytime and anywhere basis. These resources (or data) constitute what is widely known as contextual information. In these systems, there is an association between a system and its environment and the system should always adapt to its ever-changing environment. This situation makes the Context-Based Access Control (CBAC) the method of choice for such environments. However, most traditional policy models do not address the issue of dynamic nature of dynamic distributed systems and are limited in addressing issues like adaptability, extensibility, and reasoning over security policies. We propose a security framework for dynamic distributed network domain that is based on semantic technologies. This framework presents a flexible and adaptable context-based access control authorization model for protecting dynamic distributed networks’ resources. We extend our security model to incorporate context delegation in context-based access control environments. We show that security mechanisms provided by the framework are sound and adhere to the least-privilege principle. We develop a prototype implementation of our framework and present the results to show that our framework correctly derives Context-Based authorization decision. Furthermore, we provide complexity analysis for the authorization framework in its response to the requests and contrast the complexity against possible optimization that can be applied on the framework. Finally, we incorporate semantic-based obligation into our security framework.
In phase I of our research, we design two lightweight Web Ontology Language (OWL) ontologies CTX-Lite and CBAC. CTX-Lite ontology serves as a core ontology for context handling, while CBAC ontology is used for modeling access control policy requirements. Based on the two OWL ontologies, we develop access authorization approach in which access decision is solely made based on the context of the request. We separate context operations from access authorization operations to reduce processing time for distributed networks’ devices. In phase II, we present two novel ontology-based context delegation approaches. Monotonic context delegation, which adopts GRANT version of delegation, and non-monotonic for TRANSFER version of delegation. Our goal is to present context delegation mechanisms that can be adopted by existing CBAC systems which do not provide delegation services. Phase III has two sub-phases, the first is to provide complexity analysis of the authorization framework. The second sub-phase is dedicated to incorporating semantic-based obligation.