# Analysis of Authorization Framework and its Implementation

## A Dissertation Proposal

**Submitted by:**
**Pushpendra Singh Bhandari**
**CDCSIT, TU**

**Submitted to:**
**Central Department of Computer Science and Information Technology,**
**Tribhuvan University,**
**Kirtipur, Nepal**

**Under the Supervision of:**
**Supervisor: Prof. Dr. Subarna Shakya**

## 1. Introduction

Distributed Environments are touching new heights, becoming more useful, popular and more complex with the emergence of service oriented architecture and computing technologies. These technologies aim to enable large scale resource sharing. Security is a big and challenging issue in these environments as it involves the federation of multiple heterogeneous, geographically distributed autonomous administrative domains. The dynamic and multi- institutional nature of service oriented environments like grid and web introduces several challenging security issues that require new technical approaches. The framework is intended to provide a simple, powerful, flexible and scalable authorization infrastructure for services exposed in a large scale distributed environment.

Communication is an essential part of life. When we talk about the communication actually we talk about the digital communication as the internet has evolved as the new medium of communication for the digital information. This digital form of communication is different from the traditional medium of communication. In the digital form of communication the role of authentication and authorization is very important. Each and every resource is placed online and everyone has equal access to internet connection. So it may be possible that the users unknowingly or intentionally change, modify or delete the information. So every user who wants to access any resources in the network should be authenticated first depending on the requirements. Now based on the authentication the owner of the resource decide whether this user is authorized to use the requested resource or not. Every authenticated user is not necessarily authorized to use the resources. The authorization may also depend on the level of security.

With the wide use of Internet-based applications, security in distributed systems becomes a serious issue to individuals, companies and organizations. This makes computer security a necessity to all computer users. Thus, many users use a security service that can be used to protect them from others. However, security services require extra computing resources because they are time-consuming.

**Authorization:**

Authorization is the mechanism by which a system determines what level of access a particular authenticated user should have to secure resources controlled by the system. For example, a database management system might be designed so as to provide certain specified individuals with the ability to retrieve information from a database but not the ability to change data stored in the database, while giving other individuals the ability to change data. Authorization systems provide answers to the questions:

- Is user X authorized to access resource R?
- Is user X authorized to perform operation P?
- Is user X authorized to perform operation P on resource R?

## 2. Problem Definition

Authorization is a big and challenging issue. In a large scale service oriented computing environment where thousands of computers, storage systems, networks, scientific instruments and other devices distributed over heterogeneous wide area networks presents unique security problems that are not addressed by traditional client-server/distributed computing environments. The Main problems are:

- User population and resource pool is large and dynamic,
- Resources have different authentication and authorization requirements,
- Computations span over multiple domains,
- Users have different roles/privileges in different domains etc

Nowadays many organizations share sensitive services through open network systems and this raises the need for an authorization framework that can interoperate even when the parties have no pre-existing relationships.

Though there is some focus on the security but it is limited only within the authentication process (i.e., user-id/password concept only). Yet we have not reached to the Authorization process without which there is no use of authentication and security of the system.

The main objective of this work is to focus on importance of authorization to control access of the protected resources from unauthenticated users in a distributed system and to provide the core mechanisms to allow users to determine exactly which information about them is released by using the several controls and mechanisms provided by various authorization techniques and tools. One of the most widely used used automated authentication and authorization tool is Shibboleth. Finally, a prototype will be designed to give the concept of how to implement authorization in an application to have a secure access to the protected resources.

## 3. Objective

The main objectives of this study are:

- To investigate about the need of authorization systems.
- To find out the requirements for an authorization system.
- To find out about the authorization policies and its mechanisms.
- To develop the concept to solve the problem of resource accessibility by unauthorized persons by implementing the authorization framework.
- To develop a concept of multi-agent system that acts as a middleware between the user and the network-centered computing environment.

## 4. Research methodology

The research will have the following methodology.

**Literature Survey:**

In this phase, a detailed analysis of different authorizations policies and its mechanisms is done to investigate about the need of authorization systems and its requirements.

**Implementation:**

In this phase, an application named ‘X/E PST(Project Support Tool) ‘ a project management tool developed in Javra Software Nepal to demonstrate how authorizations have been controlled based on different access controls.

## 5. Expected results

After the completion of this research work, the need and requirements for authorization systems is identified and how different authorization policies and its mechanisms can be applied in distributed systems to provide simple, powerful, secured and flexible authorized systems is determined.

## 6. The estimated Schedule:

| | |
|---|---|
| Document collection | 14 days |
| Study and analysis | 20 days |
| Implementation | 10 days |
| Testing | 5 days |
| Report writing | 15 days |
| Review | 5 days |
| Final presentation | 1 day |

**References:**


- N. Papatheodoulou, N. Skalvos,IEEE Member, 2009, *Architecture & System Design of Authentication, Authorization & Accounting Services*: Proceedings of The IEEE Region 8, EUROCON 2009, International Conference (IEEE EUROCON'09),St. Petersburg, Russia, May 18-23, 2009
- 2008 IEEE Congress on Services –Part I, Martino A. S. A Model for Securing E-Banking Authentication Process: Antiphishing Approach.
- Housley R, Polk W, Ford W, Solo D. 2002. *Internet public key infrastructure, Part I*: X.509 certificate and CRL profile. Request for Comments (RFC) 3280. In: Journal of Network and Computer Applications 30 (2007) 900–919.
- Laccetti, G. and G. Schmid. 2007. *A framework model for grid security*. Future Generation Computer Systems 23, 702–713.
- Leach P, Kaler C, Dillaway Blair, Garg P, LaMacchina B, Lampson B, Manferdelli J, Rashis R, Shewchuk J, Simon D, Ward R. A Conceptual Authorization for Web Services.
- Lambrinoudakis C, Gritzalis S, Dridi F, Pernul G. Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy.
- Understanding PKI, 2002: Concepts, Standards, and Deployment Considerations- Adams C, Lloyd S, Addission Wesley.
- Saxena, A. 2004. Public key Infrastructure: concepts, Design and Deployment-. Tata McGraw Hill.