CHAPTER III

TRUST BASED ACCESS CONTROL MODEL: AN OVERVIEW

3.1 INTRODUCTION

Web applications are nowadays a strategic means for data exchange and systems integration as they afford a simple interface between a web service provider and a web service consumer. However, web services are so widely exposed that any existing security vulnerability will most probably be revealed and oppressed by hackers.

The World Wide Web (WWW) has experienced significant growth in Business organizations, individuals and government organizations. They have found that web services can offer effective, efficient and trustworthy solutions to the challenges of communicating and conducting commerce in the 21st century. As more and more enterprise web services dealing with responsive financial and confidential data turn online, the security of such web services have come under secure inspection. Compromising the security issues of these web services represents a serious threat to the organizations that have deployed these web services as well as to the users that trust these systems to store confidential data.

Hence, web services prototype faces number of new security challenges. Nowadays service provider’s who provides the service to the requester, big challenge is detecting and preventing malicious requesters or malicious behavior. In order to evade it, the service providers who allow service requesters to access the web services, requires development of access control models that can capture relevant information about a service requester at the time of access request and incorporate this information for making effective access control decisions.
An access control model for a web service is used to restrict the set of clients who invoke the operations offered by the service. There are different access control models such as Role-based access control model, Attribute access control model, Session based access control model and trust based access control model. Access control models have policies which define rules stating that only subjects with certain credentials satisfying specific conditions can interact with a web service.

This newly developed multifactor trust-based access control model introduces an enhanced trust-based access control based on multifactors such as success rate, failure rate, time out, server error, frequency of access and average time of access of web service requesters. Initially to avoid unauthenticated users, system checks SQL injection attack and IP address spoofing.

This initial identification of malicious users will reduce the time of trust-based access control model also confirms that the requester is not a fraudulent user. Once the web service requester is identified as an authenticated user, the system will calculate trust value based on the multifactor. Based on the threshold trust value, requesters will be classified as honest and dishonest users and active and inactive users. Honest and active users will be allowed to access the web services. Dishonest and inactive users will not be allowed to access the web service.

In the previous chapters, background of research, related concepts which are used to implement the access control model were discussed. This chapter gives an overview of the access control model with its architecture. It also describes all the components and their interaction with other components in the model briefly. In the coming chapters all components are described in detail.

Hereafter, this newly developed multifactor trust based access control model will be called as trust based access control model throughout the thesis.
3.2 ARCHITECTURE OF TRUST BASED ACCESS CONTROL MODEL

The following Figure 3.1 provides overall system architecture of the trust based access control model and its components interaction.

Figure 3.1: Architecture of Trust-Based Access Control Model
In the overview of trust based access control model architecture, there are two major components. They are as follows:

A. Web service requester who accesses the web service

B. Web service provider provides the service and controls the access.

The newly developed access model is located at web service provider’s access control layer to prevent malicious users. Web service, the target of service requester located at web service layer.

Most of the access control models are performing authentication and authorization processes before they allow requesters to access the target. This work also controls the access of service requesters in two major phases. They are as follows

1. Authentication Manager
2. Authorization Manager.

In this chapter, the components and their working principles are described. It assumes that requester and provider are already bound with each other for communication.

### 3.2.1 Authentication Manager

The Authentication Manager’s role is to authenticate the registered service requester’s identity. It consists of three sub modules to authenticate the particular requester. They are as follows

1. User Registration
2. SQL Injection Attacks (SQLIAs) Manager
3. IP Address Manager

The following sections briefly describe the working procedure of the authentication manager sub modules and its interaction to the authentication manager.
User Registration

User registration process is the first process of the trust based access control model. Authentication manager initially checks for new user registration at web service provider area. If the process receives request for new user registration, then the requester of the service has to register their details with their IP Address with the service provider. During the registration process, requesters will be assigned unique user id to access the web service. Consequently, new requester’s details such as user id, password, requested URL, IP Address will be stored in the registered user database. If the requester is already registered, authentication manager passes request to SQLIAs Manager for detecting SQL Injection attack.

SQL Injection Attacks (SQLIAs) Manager

SQLIAs Manager is the first process of authentication manager which is used to detect and prevent SQL Injection Attack with runtime monitoring. This module incorporates the components such as SQL scanner, XML file maker and XSchema Validator.

Authentication manager passes the request to SQLIAs Manager to detect the SQL Injection attack and takes the decision from the SQLIAs Manager’s response whether to go to the next function or deny the request. If the SQL Injection attack is identified, the service requester is denied to access the web service, by authentication manager else it sends grant signal to the authentication manager. Then it calls the next subcomponent IP address manager to check IP spoofing.

SQLIAs manager detects and prevents SQL injection based on the XML and XSchema validation. Hence, the access control model detects and prevents SQL injection vulnerabilities from the fraudulent requesters.
IP Address Manager

IP Address Manager is the second authentication process, which is used to detect and prevent the IP address spoofing in the system. This component incorporates three subcomponents. They are data filtration, user authentication and IP address spoofing identification.

This component with its subcomponent is depicted in the overall architecture. Based on web server log analysis and ingress packet filtering algorithm, it finds the IP address of the service requester is spoofed or not. If IP address is spoofed, the system sends deny signal to the authentication manager otherwise it sends grant signal to the authentication manager. Once it receives grant signal from the IP address manager, the authentication manager confirms that the requester is an authenticated user and then it forwards the process to authorization manager. The detailed description of authentication manager is given in chapter IV.

3.2.2 Authorization Manager

The Authorization Manager role is to control the authenticated requesters to access the web service by evaluating the trust level for every access dynamically using the trust manager. Based on the trust value, the requester will be allowed to access the web service. The following section briefly explains the evaluation method of trust manager and its sub components.

Trust Manager

Trust Manager is the one and only module under authorization manager, which calculates the trust value of requesters based on multifactor such as success rate, failure rate, timeout, and average time of access etc.
Trust manager incorporates the components called Trust Decision Point (TDP), Trust Management Point (TMP) and Trust Negotiation Point (TNP).

TDP checks the trust value of requester initially. If the trust value is greater than its threshold value, it allows other components to calculate the trust value otherwise sends denial signal to authorization manager.

TMP calculates the trust value dynamically and sends it to the authorization manager. This trust value is greater than its threshold value, authorization manager allows the requester to access the service otherwise it does not allow accessing the web service.

Trust manager has the process of trust value negotiation for requesters those who maintains maximum trust value consistently for a specific period and those who have failure rate due to server error. TNP is the process which takes concern about trust negotiation process. Hence, the service violation and bad client behaviors such as time out, less in access frequency leads to decrease in the trust value, whereas good behavior such as better success rate, frequent access of service leads to increase in the trust value. The detailed descriptions of authorization manager and its component functionalities are given in chapter V.

3.2.3 Registered User Data

Registered User Data is a data storage area of this access control system which maintains all registered users details such as user id, username, password, Remote IP address of last request, success rate, failure rate, access frequency, number of time out, date and time of last request, previously requested page, number of hits (entry of visited time), server error, Number of status codes ‘200’, ‘400’ and ‘408’ and other personal details of registered service requesters. Based on the status codes success,
failure and server errors can be identified by the model. Table 3.1 specifies different status codes and their description.

<table>
<thead>
<tr>
<th>Status Code</th>
<th>Description</th>
<th>Status Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>OK</td>
<td>408</td>
<td>Request Time-out</td>
</tr>
<tr>
<td>201</td>
<td>Created</td>
<td>409</td>
<td>Conflict</td>
</tr>
<tr>
<td>202</td>
<td>Accepted</td>
<td>413</td>
<td>Request Entity Too Large</td>
</tr>
<tr>
<td>203</td>
<td>Non-Authoritative Information</td>
<td>414</td>
<td>Request-URL Too Large</td>
</tr>
<tr>
<td>305</td>
<td>Use Proxy</td>
<td>500</td>
<td>Server Error</td>
</tr>
<tr>
<td>400</td>
<td>Bad Request</td>
<td>502</td>
<td>Bad Gateway</td>
</tr>
</tbody>
</table>

3.3 CONCLUSION

This chapter presented the overview of architecture and working concepts of the trust based access control model of web service access briefly. It also shows the interaction between the components in the model. The next three chapters are dedicated to detailed specification of the trust based access control model and its sub components. Thus, access control of web services is required to cross the border of security domains, and to address the movement of unknown users across borders so that access to services can be granted.