CHAPTER VIII

CONCLUSION

8.1 CONCLUSION

This Research work has presented multifactor trust-based access control model for widely used web services. The access control decision is given new focus by not asking “Who may access this resource”? But it asks “who is trusted to access this resource? In this work, it is identified that the behavior of users such as success rate, failure rate, access frequency, average time spend, time out plays important role in trust evaluation.

According to the statement made in motivation, time reducing and malicious attacks are the issues handled effectively in this work. Therefore, this work has a process called an authentication manager which checks SQL injection in the user request then checks for IP address spoofing at the initial stage of model. The authentication manager consisting of SQLIAs manager was implemented for detecting tautology type SQL injection based on XML and XSchema validation and IP spoofing controller was implemented for detecting IP spoofing based on ingress packet filtering technique. Since the authentication approach is performed at initial level of this access control model, it was found to be very effective. Comparing with previous approaches, there is a significant improvement in execution time and also in protecting the system from the tautology based SQL Injection and IP spoofing in web related logging system. So, the initial authentication processes supports to reduce the execution time and avoiding malicious users at initial level itself.

This initial level authentication process also reduces the load of Authorization manager by detecting and preventing the malicious users. Authentication manager
does not allow the users to access the web services if any issue like SQL injection or IP address spoofing is present. Hence, only authenticated users reach authorization manager which makes trust manager job easier.

Since web services are exposed to number of users, there is an issue of trusting users those who want to access the web services and manual trust evaluation system which is not possible if user’s numbers are high. Hence, this work focuses on behavior of users and effective trust policy to evaluate the trust value dynamically. Sometimes, the trust value will be decreased even though there is no issue at user side. For example, server error may causes failure in the user transaction. It is avoided by trust negotiation concept in the access model. So, this kind of Trust negotiation policy helps users to participate in the access process fascinatingly.

Since this access control model has been developed effectively based on multifactor trust evaluation with SQL Injection attack and IP address spoofing detection and prevention, this can be used for any web application and web services interaction to prevent unauthenticated users without depending specific platform. For example, the web services for ticket booking, hotel booking, etc. Since this work is developed as a loosely coupled system, it can be used in different platform. 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.
8.2 FUTURE RESEARCH DIRECTIONS

This Research work has achieved many set objectives as previously described, but still it has limitations. These limitations that shall be enhanced in future are described in this section.

In this work, trust is calculated at the level of web service provider. In case of complex web service environments like compositing web services or integrating service providers require an efficient web environment for computing the trust. Hence, an effective access control model with better trust policy management shall be implemented in future.

This model uses different factors to evaluate the trust of users. In future work shall be extended to have more factors to evaluate and negotiate the trust value of users. Hence, more users can be benefited by the system.

This work now checks only tautology based SQL injection. In future, it shall be analyzed for different types of SQL injection impact on web services security. Tampering the data is a kind of attack all web application face nowadays. In future, the process to check the tampered data shall be implemented to provide more security to the system.