CHAPTER 7

CONCLUSIONS AND FUTURE RESEARCH

7.1 CONCLUSIONS

In this research work, new algorithms have been proposed to detect and prevent the attacks efficiently. The attacks present in the literature have been surveyed and the limitations of existing countermeasures are discussed. For example, the conventional filters were designed to mitigate the attacks in fixed form of filtering approach and hence affect the system. To protect the system from the injection attacks, the self-aware message analyzing and validating algorithm against script and XML based injection attacks on Web Services have been proposed in this thesis. It filters the attack from analyzing the nature of the request and response of the communication between the client and server. Moreover, the XML based attacks are prevented in this work by XML based message validation algorithm. It is proposed as an effective way to capture the message and validate the attributes of the received XML document.

Further, the Web Services are attacked by the replay attack and spoof attacks. To protect the Web Services from these attacks a dynamic nonce based authentication scheme has been proposed in this thesis to secure the Web Services. This approach produces a dynamic random nonce for verification at the time of accessing the Web Services. The system has been tested with a large set of attacks to check its defending capability. Also, the performance analysis has also been conducted with large number of requests.
From that results, it is observed that the system is capable of performing requests in real time. In addition, it has been designed for the system with low configurations. Hence, it gets system parameters to generate random nonce.

7.2 SCOPE FOR FUTURE RESEARCH

The system can be extended further to provide a feature to get the dynamic nonce and other keys using Kerberos token for mult-business Web Services in the federated environment. In addition, this research work can be extended to solve any type of new attacks (0-day attack). In stead of using validation approach, it can be extended to use a hardening approach.