ABSTRACT

The users are accessing the web applications in the areas such as education, Information Technology and communication, entertainment and commercial applications. Web applications are weakly secured against variety of attacks such as Denial of Service, Brute Force attack and Session Hijack attacks. Session Hijack attack is the most severe attack to the web applications. Most of the web applications involves in creating the session with the client. Hyper Text Transfer Protocol (HTTP) is the default protocol responsible for establishing the session in the application layer. Session hijack attack is easy to launch and it is difficult to detect.

To prevent the Session Hijack attacks in web applications a prevention model is proposed using Message Authentication Code (MAC) appended Session ID. The integrity of the session ID is tested by executing the various attacks and the results proved that MAC appended Session ID is completely prevents the session Hijack attacks in web applications.

To prevent the Session Hijack attacks in web applications a prevention model is proposed using encrypted Session ID. The proposed encrypted session ID is completely prevents the Session Hijack attacks. Session key authentication and distributed session ID is proposed to prevent the session hijack attacks in healthcare web applications. A Four Tier Validation System is proposed to prevent the Session Hijack attacks by defending the Cross Site Scripting attacks in web applications. Client side inputs are validated in the first tier and the web server configurations are validated in the second tier. In the third tier, malicious Hyper Text Markup Language (HTML) scripts and Java scripts are validated. In the fourth tier, http headers and hidden form fields are validated. The proposed four tier validation system completely eliminates the cross site scripting attack and thus prevents the Session Hijack attacks in web applications.