People seeking medical attention go in search of medical centers and specialists. For them time is vital as they search for resources, the information should be available with minimum latency. With the advent of wearable computing and ubiquitous computing Context-Aware Web services can be available with much ease, it enables users to retrieve information with relation to their context. While providing several benefits, although web services technology has been facing serious threats like prefix hijacking and interception in the Internet due to a man-in-the-middle attack which compromises privacy of the user. The objective of this research work is to provide a secure framework for Context aware web services using access control mechanisms. It was found web services are prone to data theft and malicious attacks, Access Control Mechanism is introduced in the framework to provide a secured architecture where the privacy of the person accessing the web service will be preserved. The proposed architecture provides an end-to-end security by accomplishing the security properties such as user authentication, authorization of web services, message confidentiality, data integrity and non repudiation. Hence, there is a need that arises to design a security system for context-aware web services with the support of
end-to-end security in business services between the service providers and service requesters thus providing a secure user experience

References


Index Terms

Computer Science Security
Keywords

Web Services, Web engineering, Context-aware, access control, security, privacy.