# Secure Communication and Access Control for Web Services Container

**ABSTRACT**

Security is a crucial aspect in any modern software system. It is uttermost important for secure communication and access control in in-house business applications which are couple over the Internet using Web services. This paper firstly creates Web services container for wrapping COTS components (in-house business applications) toWeb services. Then, a Web services security framework (WSSF) is presented to offer an effective solution forsecure communication and access control of Web services container. The proposed framework focuses on addressing problems in two aspects: (1) Web services secure communication, i.e., the ability to send security tokens as part of a SOAP message to authenticate users, to provide message integrity, and message confidentiality; (2) authorization and permission delegation, i. e., the ability to define dynamic permission, and to assign attribute-based role. Finally, the paper gives prototype system StarWebService and proves the feasibility and validity of WSSF framework

# A secure framework for web service interaction

## ABSTRACT

Automated composition and interaction of semantic web service is one of the most promising challenges in semantic web service research area, in which security research on service composition has attracted more attention. In this paper, we present a framework of Action labeled Kripke Transition System, which can abstract interaction behaviors between distributed web service and translate them into logic symbols, then propose asecure conversation mode with constraints based on WS-Trust and WS-Secure Conversation to ensure the security of service interaction. Finally, the security interaction among semantic web services can be easily verified by deterministic propositional logic.

# Secure E-business Transactions by Securing Web Services

## ABSTRACT

Due to the popularity of internet and the growth of e-business, the world became very small. Everyday people are using internet as the medium of transaction of millions of dollars from one account to another. The webservices are playing very crucial role in online transactions. That's why we have to think about the security of our entire transactions as well as web services. Web service transaction should be of major concern. Many technologies available which are providing web service facilities, for example java, .net etc. There are various options available to make web services secure. We can choose any options from protocols based, platform based or message based security. There are securities which can be IIS based, Asp.net based and SSL etc. Various threats to web services and e-business are also present. Threats like unauthorized access, alteration, disclosure of very important data, message reply etc. Anyone can hack the WSDL information and can get into downloadable files. While designing and developing the web services we have to think about code access security. In this .NET technology is being used for most of the examples. In this paper, the possibility of reducing the business cost through e-business is being explored.

# Techniques of Secure Web Service and its Implementation

## ABSTRACT

The security of web service is a key to its successful application in the business field. In order to satisfy the basic needs of e-business, this paper puts forward a kind of secure web service architecture, which includes secure communication protocol, data encryption, data integrity, authentication and user access control etc. It provides a rapid, convenient, and transparent data security service for Browser/Server applications.

# Taking steps to secure Web services

## ABSTRACT

Despite the promise, Web services present network administrators with a thorny problem: as network security becomes an increasing concern, Web services open up networks by letting outside users access databases, applications, and internal users. Traditional security techniques - such as virtual private networks or securesockets layer (SSL) technology - cannot secure the large number of transactions that Web services can perform in a short time. Meanwhile, basic Web services transactions are unencrypted and unsecured, which creates the potential for disaster. It is thus important for Web services technology to have its own security mechanisms. In fact, industry observers have said the biggest obstacle to wider adoption of Web services has been security concerns. With this in mind, researchers are developing and implementing several Web services security approaches.