http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 11 (2): 241-247, 2012
ISSN 1812-5638 / DOI: 10.3923/itj.2012.241.247

Research of Web Service Security Model Based on SOAP Information

Shujun Pei, Deyun Chen, Yuyuan Chu, Qingfeng Xu and Shi Xi
College of Computer Science and Technology, Harbin University of Science and Technology, Harbin 150080, China

Abstract: Web Services is a new distributed computing model. It has the characteristics of loosen coupling, cross platform, dynamic and openness. It can accelerate integration of different kinds of governments, business and enterprise systems, reduce cost and improve benefit, but they also lead to many security problems. The security of Web services deeply influences its development and is also one of the main reasons why Web Services has not been adopted widely. Their communication requirements to ensure the realization of end-to-end security and confidentiality of Simple Object Access Protocol (SOAP) information transmission, but traditional programs such as the SSL transmission can not meet demand. In this paper, we analyzed the representative solutions to web service security in detail. Proposed a security model and implement the model in J2EE platform by using inventory Management System, ensure end-to-end security of SOAP information transmission.

Key words: Web service, SOAP, XML, security model, end to end

INTRODUCTION

Web Service built on a set of XML-based standard protocol is a self-contained, self-described, component-based application. Web Service as a new distributed computing model, is the effective mechanism of data and applicative integration on Web and also the first choice of emerging computing technology, such as grid computing and cloud computing, etc. Web Service has the platform-independent, dynamic, open and loosely coupled characteristics which bring great convenience to enterprise application integration. But this makes it face many unique security problems. One of the major reasons that prompt it enter into a large-scale application stage is that the security of Web Service's crucial impact on its applicative prospect. Thus, an in-depth study of Web Service Security has both important theoretical significance and application value. Web Service, the service request and response SOAP messages are based on the form of packaging and delivery, SOAP Web Service is the core of the message. In Web service, service request and response are all packaged and delivered by SOAP messages which are the core of Web service. Therefore, Web service's basic security request is to protect the confidentiality and integrity of SOAP message (Tatsubori *et al*., 2004). SOAP messages can be transported based on a variety of protocols (such as HTTP, SMTP), the transfer process may span a multiple of intermediate nodes, TLS/SSL can only ensure the point to point transmission security. When an intermediate node is not credible, it can't guarantee end to end security of SOAP message, there is the need to provide SOAP message with security which is not rely on low-level mechanism, independent message layer. The security factors of information transmission of SOAP message on the Internet are: how to identify the identity of the two communicating parties (identification and authentication), how to ensure that the sent message without the reach of unauthorized persons (data confidentiality), how to ensure that the message received from others are not modified (data integrity), how to ensure that legitimate users operate within the specified range (authorization and access control), how to ensure that the sender can not deny he sent a message (no deniable). In order to ensure the transmission security of SOAP messages on the Internet, many scholars and organizations have joined the study of security policies. A variety of security standards had been put forward which brought about the breakthrough of Web Service security (Bucker , 2007).

WEB SERVICE SECURITY-RELATED SPECIFICATIONS

XML encryption: XML Encryption Syntax and professing is a specification developed by a working group (XML Encryption Working Group) of W3C. This specification describes the process of data encryption and XML representation of the encrypted results. The XML

Corresponding Author: Shujun Pei, College of Computer Science and Technology, Harbin University of Science and Technology, Harbin 150080, China

Encryption is widely used, it supports any digital content encryption, encrypts the whole document or one of the elements in the document, or even the content of an element. It ensures that confidential data in the transmission process not be acquired by a third party, implementing the confidentiality of data transmission (Sidharth and Liu, 2007).

XML signature: XML Signature Syntax and Processing is a specification developed by a collaboration working group (XML Signature Working Group) between W3C and IETF. This specification describes the XML representation and calculation of digital signature and digital signature verification process of XML representation. To ensure the data integrity, reliability and non-repudiation, digital signatures ensure reliable data exchange capabilities of Web Service (Talib *et al*., 2004). What's more, XML signature can have a choice of XML data signatures which can ensure both the change in information head and the end to end integrity of SOAP parameters.

Security assertion markup language: Security Assertion Markup Language, (SAML) is the XML framework of exchange authentication and authorization information. It defines syntax and semantics that XML-encode the authentication, attribute and authorization information as well as the transfer protocol of security information. Safety information is expressed by the form of statement. A statement contains a number of different statements on authentication, authorization and attributes (Yang and Li, 2010). Statement is processed by the SAM authority and the clients can send response statement to the SAML authority. The exchange of security information typically occurs in the case that interactive applications are not in the same authentication and authorization domain. SAML allows the joint system development; it can achieve integration and information exchange among different security systems, meeting different needs of treatment from single sign-on to the authorization service.

XML public key management specification: XML Public Key Management Specification (XKMS) is a W3C proposal, originally co-sponsored by Microsoft, Version and Web Methods. It specifies a protocol for the registration, distribution and public key processing which provide direct support to XML encryption and XML signatures (Yan-Ping and Zeng-Zhi, 2007). Web Service application program can simply provide XKMS service with <ds: KeyInfo> elements to locate and obtain the key value referenced by this element or verification and validation of the key. XKMS draw up a convenient and standard mechanism for the access to integrated public key infrastructure. It defines the key and certificate management standards, including registration, distribution, revocation and other operations, allowing customers to obtain key information through a Web service, improving the security of network data transmission combined with XML encryption and XML digital signature specification.

WS-security specification: WS-security specification aims to enable the application program to construct secure SOAP message exchange, providing end to end security. Main function is to describe how to attach signature and encryption header and the security token to SOAP message. The specification is flexible and it is designed in the scope of a variety of security models such as PKI, Kerberos, etc. As the basic protection to the Web service, it supports multiple security token formats, multiple trust domains, multiple signature formats and encryption technology. Specification provides three main mechanisms: security token transfer, message integrity, message confidentiality. In practice, whether it is XML Signature, XML Encryption, Security Assertion Markup Language SAML, or Key Management Specification XKMS, having the limitation that they only meet some of the security needs. WS-Security has developed complete security standards, but these mechanisms alone can not provide complete solution for Web service security. Specifications required the joint use with other Web Service extensions and higher-level protocols that specified to application programs to accommodate a wider range of security models and security technology (Mansourian *et al*., 2008). This paper designed a Web Service security model which can meet the demand for secure transmission of SOAP messages.

WEB SERVICE SECURITY MODEL DESIGN

Role design of security model: The security model consists of five roles: service requester, service provider, UDDI registry, XKMS server and SAML server. Service requester is the party to apply for service and it has the access to services through browser, Web Service, components and other SOAP clients. Service provider is the provider of Web Service and it offer resources to legal SOAP requester, verifying the secure SOAP message of service requestor. After authentication, authorization test, it determines whether they should be given the access to services. UDDI Registry stores service description information by category, it is a public registry which is used to register and search the Web Service. XKMS server provides key registration, location, authentication and other services, using for the processing and managing PKI-based encryption, signature keys. Through

these services, it shields the complexity of using the PKI to the service requester and service provider, ensuring mutual authentication between requestor and provider and establishing mutual trust. SAML management organization is the right management organization. It deals the system access control and authorization in the form of SAML assertions, including user authentication information and the related authorization information. As security tokens, SAML assertion states the user's security information (Thelin and Murray, 2002). SAML assertion issued the assertion to the service requestor, transferring its trust to the user and the user's attributes, authentication, authorization information and then requestor sent the assertion to service provider. SAML assertions may be a third-party trust service, the verification service which is located in the same institution with requestor or the requestor itself.

Building web service security model: Specific procedures of web service security model are shown in Fig. 1.

The entire process of security model system is as follows:

Step 1: The service requester and service provider registries certificate to their XKMS server, respectively

Step 2: The process of service requester to the SOAP message is as follows:

- Service requester obtains the certification offered by service provider from XKMS server
- The service requestor logs on to the SAML server, after the authentication, it removes the access rights from the policy repository which is appropriate to the logger, generating SAML assertions (including authentication, attribute, authorization assertions) and adds to the SOAP message header as the user security token
- To add security attributes in SOAP message header is to prevent the replay, a third-party's attacks. It contains the time stamp, sequence number, sender and recipient four basic properties and it can also extend properly according to security requirement
- To encrypt the SOAP message with the public key in the service provider's authentication book; to encrypt the feature with the XML encryption part, only to encrypt the confidential SOAP message, but not to encrypt the Header part of SOAP message. Chain encryption is used here to encrypt the confidential information, combining the asymmetric encryption algorithm and the traditional symmetric encryption algorithm together. Service providers generate a random generated key (different for each encryption), using symmetric algorithm to encrypt the message in plain text and to encrypt the key with asymmetric algorithm

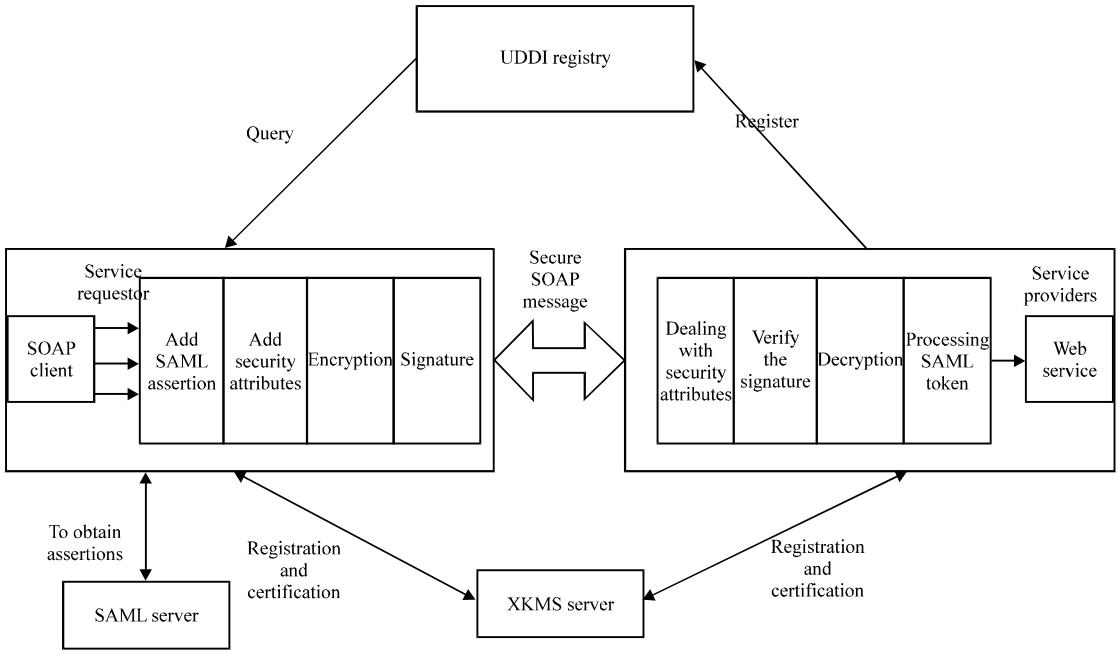

Fig. 1: Web service security model

- To package the requestor's certification in SOAP message and send it to the service provider

Step 3: Service providers' security process to SOAP message is as follows:

- Service provider receives the message, verifying and dealing with security attributes, checking and determining whether it should be replayed and if the corresponding receiver and sender are correct
- Service provider verifies the validity of the certificate to the XKMS server according to the certification in the message, confirming its validity and then gets the public key to verify the signature
- The service provider acquires the requestor's random private key by the combination of asymmetric encryption algorithm and its certified book and then acquires the random key by the use of symmetric encryption algorithm to conduct decryption
- To decide whether the requestor has access to the resources according to the authority information in SAML assertion. If it is permitted, meeting the requestor and send SOAP response information. If not, deny the requestor's requests

An analysis on communication model's security performance: There are security mechanisms and norms XKMS, PKI, SAML, XML Signature, XML Encryption in security model. The SOAP message after procession by these security technology can guarantee the end to end data transmission, including authentication, data integrity, confidentiality, non-repudiation and authorization these security features (Tang *et al*., 2006).

Authentication: XKMS, SAML and XML Signature in communication model all provide support for authentication. XKMS verifies the identity of service requestor and service provider by providing certification. By providing assertion that storages verification, it verifies the identity of the logger. XML signature signs the sent SOAP message by the sender's private key so as to verify signer's identification. These security mechanisms prevent the access to the resources of the non-authorized users.

Data integrity: This security feature can be implemented by the XML signature. If a third party intercepted the signed message, it may modify the message content. But because of the unknowing of the sender's private key, it can not calculate the revised summary value. The recipient can learn that the message may be tampered during transmission so as not to trust the message and then the data integrity of message transmission can be ensured.

Confidentiality: the confidentiality of the message transmission can be achieved by using XML encryption. The encryption mechanism combined the symmetric key with the asymmetric key to encrypt the SOAP message partly and selectively. Message sender randomly generates a random key, it encrypts the message clearly with symmetric encryption algorithm and then to encrypt the key with asymmetric encryption algorithm. This chain encryption would achieve both confidentiality of the symmetric encryption algorithm and the quickness of the asymmetric encryption algorithms, thus ensuring the message confidentiality in message re-transmission.

Non-repudiation: This property refers to a party's undeniable of the information sending behavior who participates in the communication exchange after submitting information and identity verification. This security feature can be achieved by XML signature. After the registration of the certificate, the sender need the corresponding private key signature to send the message and after receiving the message the receiver uses the public key of the certificate to authenticate the sender.

License: SAML can achieve the authorization function. The logger generates SAML assertion after the certification, storing information on access to resources (Hanna and Abu Ali, 2011).

WEB SERVICE SECURITY MODEL EMPIRICAL

Based implementation of the inventory management system: According to the Web Service security model in this paper, we take the inventory management system of mobile phone factory for example to authenticate the application effect of this model. Mobile plant, major parts plant and retailers maintain a long-term cooperation. However, because the previous operation mode does not grasp the state of the supply chain of upstream and downstream, leading to over production and excess of inventory for not knowing the distributor's sales conditions. Or because there is no news of the supplying status of the upstream supplier, leading to the amount of original fittings is lack of the need of production, in short supply. We use Web Service technology designed an inventory management system to keep production

schedule of the ordered parts and tracking the sales of the major retailers. Through analysis of these data, we can develop optimal production plan and manage the inventory better.

Supply and inventory management system consists of: landing module, parts procurement module, sales management module, inventory management modules, production planning module. Among which, the production planning module and inventory management module called the Web Service offered by suppliers and vendors. After the corresponding WSDL document, it packages the required business into its own system and makes appropriate production plan and inventory management. Parts suppliers offer the price of parts products, ordering and the inquiry services for the parts' production schedule. Retailers provide sales information services outside, including volume of merchandise, sales price, weekly sales, number of returns or the quantity of repair, etc. To package these services into Web service is for secure communications. The use of the above-mentioned security model adds corresponding functions to it and guarantees the communication security in Web service call. Specific security model is shown in Fig. 2.

The system is developed in J2EE platform, based on SOAP containers XFire. Service requesting side uses Tomcat server, service providing side uses Weblogic server. In supply and inventory system, before sending the SOAP request information to service providing side, it pads information into the SOAP message header and encrypt the SOAP message body via SAML assertion processor, encryption processor, signature processor. Be serialized; re-generate provider side of the SOAP message service. After receiving the SOAP message, the service termination side gets the SOAP message through verifying and decrypting the processor by signature, conducting permission judgment. If it meets the permission, then it can response accordingly. If not, the result is refuse. The security processing process of the return of SOAP message to supply and inventory system is similar with that of service request side. The concrete realization of the process is shown in Fig. 3.

Comparison between the two versions of before and after processing of the SOAP message: Body information in SOAP message before security processing

```
<soap: body>
<sell xmlns="http://com.gyl.sellserver">
<days>30</days>
<model>v800</model>
<price>1500</price>
<amount>
<sellamount>70</sellamount>
<backamount>0</backamount>
<repairamount>1</repairamount>
</amount>
      </Sell>
</soap:Body>
```

Body information in SOAP after security processing:

```
<Soap: Body>
<Sell xmlns="http://com.gyl.sellserver">
<days>30</days>
<model>v800</model>
<price>1500</price>
<sellamount>
<xenc:EncryptedData Type="http://www.w3.org/2001/04/
xmlenc#Content"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
```

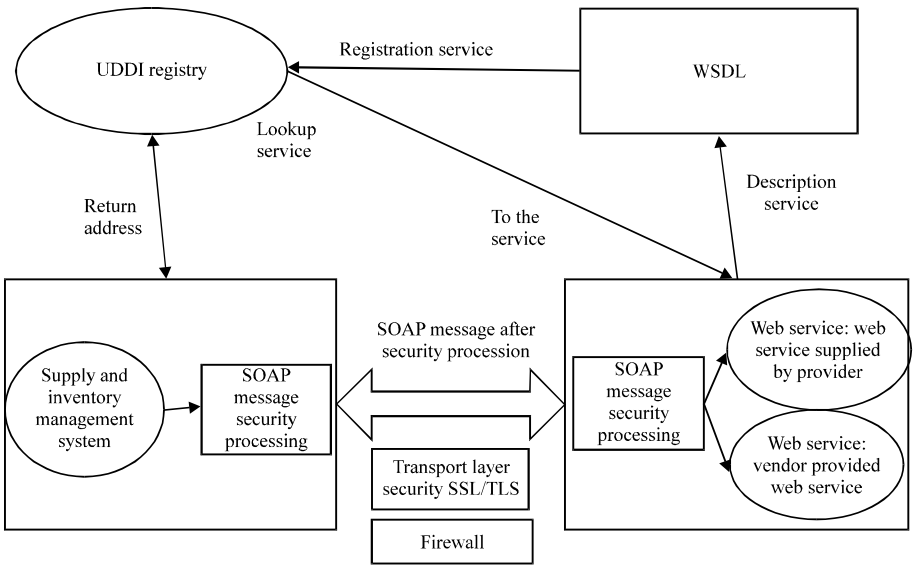

Fig. 2: Security model of inventory system

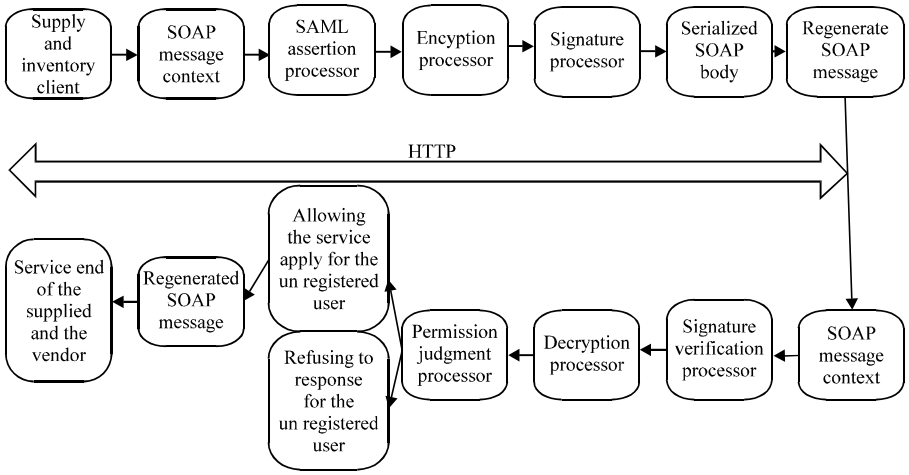

Fig. 3: SOAP message security processing

```
            <xenc:EncryptionMethod
      Algorithm="http://www.w3.org/2001/04/xmlenc#tripedes-cbc" />
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <xenc:EncryptedKey>
      <xenc:EncryptionMethod    Algorithm="http://www.w3.org/2001/04/
      xmlenc#rsa-1_5"
/>
      <ds:KeyInfo>
      <ds:KeyName>SELL UYO RXJ Key</ds:KeyName>
      </ds:KeyInfo>
      <xenc:ClipherData>
      <xenc:ClipherValue>
      GPSY7@BX3E53;JG0GOXODTZO;95;QBV@P2VR2?T?=I;[;HS
      5J@CSH=H4DC7TMQ4L?Y
PLG;7OFZN:@UBTK>9CC>UP@;>;MCE>FHSG2G5GMYKFT6=[:L
7MG0=J@AI8FTXYSEJ:JTTY[P0M1JW01?2
      </xenc:ClipherValue>
      </xenc:ClipherData>
      </xenc:EncryptedKey>
      </ds:KeyInfo>
      <xenc:CipherData>
      <xenc:CipherValue>
      MVSX5XLA6308CGH3B:Q1LFM@XJ;U4HP;=4H0ZL5USP7Y[
V94HMJZRN63;5AVAKVM@61U[BOJA24R@39DQTAR>X?CH4A0?
Z53;3A
      </xenc:CipherValue>
      </xenc:CipherData>
      </xenc:EncryptedData>
      </sellamount>
      <backamount>0</backamount>
      <repairamount>2</repairamount>
      </Sell>
</soap:body>
```

The contrast between non-encryption and encryption of the SOAP message key elements can be seen above. In which, the chain encryption method is use to encrypt the SOAP message which is characterized by jointing the symmetric encryption algorithms DES and asymmetric encryption RSA together. It is a good combination of the confidentiality of symmetric encryption and the convenience of non-symmetric. The following is a comparison provided by the vendor between non-encryption and encryption of the SOAP message of the sales information Encrypted Data element represents encrypted information, ds: KeyInfo indicates the key information, EncryptedKey elements represents the symmetric key after using the asymmetric encryption algorithm.

Table 1: The comparison before and after processing

Data flow	Before	After
Request	763	10987
Response	759	7365
Header	195	433
Body	570	13776
Time	0.3158	17.7636

From the above two comparisons of SOAP message, we can learn that the volume of SOAP context after security processing send by the client is usually wider than that before security processing. In Table 1, the data amount and time when communicating between client and server before and after security processing is shown. Data in the table are the average after many times of measurements. The design of Web Service security model achieves a secure Web Service environment compared to the original one. It has a certain increase in data amount and time span, but it is improved in terms of security.

CONCLUSION

Security is the major issue in deploying Web Service and the basis of Web Service security is the security of SOAP messages. In this paper, a convenient, flexible and ease expanded Web service security model is constructed according to the existing security technologies and standards. It is security model integrated and constructed by XML encryption, XML signature, XKMS, SAML such technologies and realized with the participation of supply

and inventory management system on J2EE platform. The model improves the security of Web Service communications, ensuring the confidentiality, integrity, non-repudiation of Web service information in communication, integrity, non-repudiation while achieving the authentication and authorization to the users. Of course, Web Service security is multi-layered, multi-faceted. Making Web service security policy that is appropriate to different security domains, achieving the security of Web Service in a wider field will also be the focus of future research.

ACKNOWLEDGMENTS

This study is supported by high and new technology industry foundation of Harbin Grant by No. 2008FG02CG201.

REFERENCES

Bucker, A., 2007. Understanding SOA Security Design and Implementation. 2nd Edn., IBM Redbooks, Nebraska, USA., ISBN: 9780738486659, Pages: 478.

Hanna, S. and A. Abu Ali, 2011. Platform effect on web services robustness testing. J. Applied Sci., 11: 360-366.

Mansourian, A., M. Farnaghi and M. Taleai, 2008. Development of new generations of mobile GIS systems using web services technologies: A case study for emergency management. J. Applied Sci., 8: 2669-2677.

Sidharth, N. and J. Liu, 2007. A framework for enhancing web services security. Proceedings of the 31st Annual International Computer Software and Applications Conference, July 24-27, 2007, Beijing, pp: 23-30.

Talib, A.M., Y. Zongkai and Q.M. Ilyas, 2004. Modeling the flow in dynamic web services composition. Inform. Technol. J., 3: 184-187.

Tang, K., S. Chen, D. Levy, J. Zic and B. Yan, 2006. A performance evaluation of web services security. Proceedings of the 10th IEEE International Enterprise Distributed Object Computing Conference, October 25-29, 2006, Hong Kong, pp: 67-74.

Tatsubori, M., T. Imamura and Y. Nakamura, 2004. Best-practice patterns and tool support for configuring secure web services messaging. Proceedings of the IEEE International Conference on Web Services, July 6-9, 2004, San Diego, California, USA., pp: 244-251.

Thelin, J. and P.J. Murray, 2002. A public web services security framework based on current and future usage scenarios. Proceedings of the International Conference on Internet Computing, June 23-27, 2002, Las Vegas, Nevada, USA.

Yan-Ping, C. and L. Zeng-Zhi, 2007. E-WsFrame: A framework support QoS driven web services composition. Inform. Technol. J., 6: 390-395.

Yang, H. and Z. Li, 2010. Improving QoS of web service composition by dynamic configuration. Inform. Technol. J., 9: 422-429.