INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Web Services: The Analysis of Service Oriented Architecture, Security Issues and Its Challenges

Punyaban Patel[1], Bibekananda Jena[2]

[1]*Department of Computer Sc. and Engg., Malla Reddy Institute of Technology, Secunderabad,*
[2]*Department of ECE, Anil Neerukonda Institute of Technology & Sciences, Visakhapatnam*

Abstract: Web Service is relatively new and a relevant area. The security issues of Web Services in a distributed environment are a major concern of research. The of research both in industry as well as in academia. The present work is mainly focusing on security issues of Web Services and its challenges. In this paper, a study on the existing standards and protocols such as the service oriented architecture of the Web services, h te role of XML, WSDL service provider facing a lot of problems when it provides users to avail the Web services. So, the Web service security is one of the thrust areas, SOAP, and the UDDI in the Web services, security issues with its challenges is carried out.
Keywords: World Wide Web(WWW), Simple Object Access Protocol (SOAP), Security, eXtensible Markup Language (XML), Web Services Description Language(WSDL), Web Services, Universal Description Discovery and Integration (UDDI), Hyper Text Transfer Protocol (HTTP).

I.   INTRODUCTION

The Web service is a software entity that has been designed for interacting and communicating between m/c-to-m/c through an agent in a computer network, as well as, to be accessed by other applications such as online banking system, online railway, buses or air ticket reservation system. The agent is a piece of s/w or h/w which sends and receives messages between m/c using standards-based web technologies, such as, HTTP and XML-based protocol messaging including SOAP and WSDL. The agent may be written in different programming language with the same functionality. Web services are independent in terms of hardware, programming language, and operating system used. This means that, although, the applications written in different types of programming language and running on various platforms can seamlessly exchange data over intranets or the internet using web services.
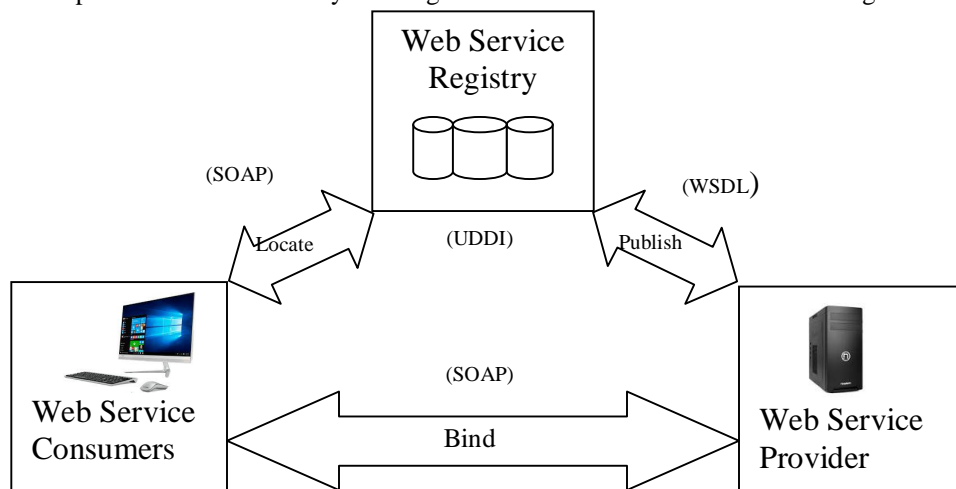

Figure 1: Service Oriented Architecture

The Web services has been gained power by XML, WSDL, SOAP, and UDDI technologies [1,2,3,4,5,6]. Before building a Web service, the developer defines it in the form of a WSDL document which describes the service's location on the Web and the functionality provided by the service. Then the information about the service will be entered in a UDDI registry, which allows Web service consumers to search for and locate the services they need. This step is optional but is beneficial when a company wants its Web services to be discovered by internal and/or external service consumers. Based on information in the UDDI registry, the Web services client developer uses instructions in the WSDL to construct SOAP messages for exchanging data with the service over

HTTP [7,8,9]. The service oriented architecture of Web services is shown in Figure 1. The service oriented architecture of Web services consist of three components. These are (i) a registry, which acts as a broker for Web services, (ii) a provider, which can publish services to the registry, and (iii) a consumer, which can then discover services in the registry[10].

This paper has been structured as in section 1: about the introduction, section 2: describes the role of XML (eXtensible Markup Language), section 3: WSDL (Web Services Description Language), section 4: SOAP (Simple Object Access Protocol), section 5: UDDI (Universal Description Discovery and Integration), section 6: Web service security, section 7: Web services Challenges, and finally section 8: gives about the conclusion of the paper.

A. XML (Extensible Markup Language)
The XML is a WWW association/consortium specification which describes a meta-language for labeling data and a key technology requirement which appears in many places[20]. In XML applications, data is described by surrounding it with customizable, text-based tags that give information about the data itself as well as its hierarchical structure. Because XML syntax consists of text-based mark-up that describes the data being tagged, it is both application-independent and human readable. This easiness and interoperability have helped XML achieve widespread acceptance and adoption as the standard for exchanging information between heterogeneous systems in a wide variety of applications, including Web services. The XML forms the basis for all modern Web services, which use XML-based technologies to describe their interfaces and to encode their messages. WSDL, SOAP, and UDDI all use XML-based messaging that any machine can interpret [11,12,13] .

B. WSDL(Web Services Description Language)
The WSDL is an XML-based format which describes the functionality of Web services, the operation it will perform and how to access them[4]. Before using the Web services by the user, one has to interpret the WSDL files to know the information about the address location of the service with its operations. So, the WSDL turns into the initial interface of the Web service, and then it provides all the information to the user in a standard way to interact with the service. A user can know how and where the service can be accessed and used, the communication protocol support, the operation with its message format through the WSDL [9,14]. The WSDL is an integral part of UDDI.

The Web service acts as a contract and agreement between Web service client and server which has been described in WSDL document. By adhering to this contract and agreement, the service provider and the consumer are capable to exchange data in a standard way, nevertheless of the underlying platforms and applications on which they are operating.

C. SOAP(Simple Object Access Protocol)
The SOAP defines a standard communication protocol specification for XML-based message exchange by using different transport protocols, e.g. HTTP, SMTP and FTP. It offers a simple, standards-based encoding scheme with its own format for sending XML messages between applications15. The SOAP can handle simple and compound type of data. Web services use SOAP to send messages between a service/server and its client(s). The SOAP messages are possible to send between clients / users irrespective of computing platform and any programming language due to the support of HTTP protocol by all browser and server. This characteristic shows that the Web service is an interoperable. The message format has been described in WSDL.

D. UDDI(Universal Description Discovery And Integration)
The UDDI has been designed for managing business related information[6]. On the basis of its specification, the organizations can store, update and share information among the parties. The UDDI uses WSDL for describing interfaces to web services communicate through SOAP, Java RMI protocol and which is an open framework and platform-independent. It is a specification for creating an XML-based registry that lists information about businesses and the Web services. The private / public registries is supported by UDDI. The developers can questions a UDDI registries for a service and also design their Web services clients to receive automatic updates made about any changes to a service from the UDDI registry[16,17,18].

II. WEB SERVICE SECURITY
The Web service security wants to be concerned with the following features [4,15,19,20]:

A. Privacy is a major concern of Web service deployment. At the time of service interactions, the private / personal data or confidentiality in business (e.g., product preference, shipping address, date of dispatch / delivery, or billing information) might not be intentionally released8. The old / conventional privacy protection mainly relies on the restriction of social values and law

enforcement. The emerging technologies for privacy preserving in Web services include data filters, digital privacy credentials, and mobile privacy preserving agents.

B. Integrity and non-repudiation refers to the safeguard of the information being tampered by others, e.g, putting digital signatures on the messages. Also, making sure that a message remains unchanged during transit by having the sender digitally sign the message.

C. Confidentiality and Privacy is to keeping information secret using XML encryption technique to ensure that information is open only to authorized recipients, for example, a Web service request or an email, as well as the identity of the sender and receiver parties in an intended to be kept secret manner. Confidentiality and privacy can be achieved by encrypting the content of a message and obfuscating the sending and receiving parties' identities encrypting the message.

D. Authorization (or Access Control) is to check whether a user is authorized to perform a requested action or granting access to particular resources based on an genuine user's entitlements where each entitlement are defined by one or several attributes.

E. Non-Repudiation is to not reject the message by using digital signature in order to guarantee non-repudiation. The specification permits variety of signature format, multiple trust domains and the encryption technique.

F. Authentication is used to verify a claimed identity something like credentials issued by a trusted authority such as a passport (real world) or a smart card (IT world), a shared secret such as a password or biometric information.

III. WEB SERVICES CHALLENGES

The Web services to achieve the desired aim or result, there are many technical challenges that have to be face. Out of these, many of them are related to the open, averse environment in which they can continue to exist. There are some of the issues have been discussed in this section [6,15,20]

A. Discovery

It means to improve the retrieval performance for satisfying customers' needs without considering the length of the response time for which many services have been discovered. But, the researchers are giving more importance on automatic discovery of the web services. The main theme of the discovery of web services consist of two parts, that is (a) the researchers are giving more efforts on caching and indexing of files systems for improving the response time and, (b) the interface to exhibit openly by discovery or search engines assumes that requests are fully mentioned in terms of a well-defined or clearly stated interface and its categorisation in terms of i/p, o/p and preconditions. Many researchers have been using AI techniques, graph-based approaches and optimization techniques to improving the response times and search engines and indexing. The WSDL and UDDI are two new standards that have been explained this problem.

B. Reliability

It represents the degree of competency of sustaining the service and the quality of service. Also, it refers to the guaranteed and systematic i.e properly sequence deliveries of messages which will be send and receive. The Web services are reliable when it responds & acknowledge the requests, communicate and deliver exact messages between the authorize sender-receiver or client-server. The reliability can be improve by eliminating when it goes off-line, different attack to network or network failures.

C. Security

Many services are available which are using encryption techniques during communications with proper authentication. The basic security can be obtained by using HTTP (Hyper Text Transfer Protocol) over SSL (Secure Socket Layer) i.e https, but distinct services require a higher level of coarseness. The security has further added significance and importance because its call / requests occur over the publicly available Internet. Also, the service providers can have various techniques & approaches and the levels of offering security based on the service requestor or users.

D. Transactions

The transaction in DBMS, called traditional transaction, complete in two-phases i.e. commit () and rollback(). It commit (commit ()) the transaction i.e. save changes made in database during transaction and rollback(rollback()) the transaction i.e. set the database to its original stage. During the transaction all of the participating resources are gathered and remain locked until the entire transaction can take place, at which point, the resources are finally released. This approach works fine in a closed environment where transactions are short-lived, but doesn't work well in an open environment where transactions can span hours or days. An alternative scheme has been supported by Microsoft, called compensating transactions, in their new XLANG system for distributed business

processes. The extensive research is going on to integrate the traditional transaction and compensating transaction to improve the quality of service.

E. Scalability

It means is that how speedily the web services can be increase its capability to meet the expectation of the end-users. For achieving the above we can move to more powerful server or by adding multiple number of servers result in increasing cost. Although, the overall cost will be increase but it will gives benefits in reliability, flexibility and performance, which cannot be apprehended in a single-server arrangement.

F. Manageability

It can be defined as a set of abilities for determining the presence, availability, performance, health, usage, configuration and the control of a Web service within its architecture. It denotes that the Web services can be accomplished by the help of Web services technologies. The Web service manageability is consist of three component such as (i) Concepts summarizes the scope & definitions, (ii) Specification initiates by presenting the general concepts about the manageability model, and (iii) Representation document tells about the interface definitions on the basis of the model. Also, the researchers are going on in-depth study on the kind of mechanism require, functions and properties of the different parts of the system and the way of coordination among the various Web services[21].

G. Accountability

Accountability in the field of Web services talk about the responsibility, commitment or, and obligation that a number of persons, or establishments / organizations accept for the implementation and accomplishment of a service. This obligation includes: answering, explanation with proper justification, providing fulfilment of that responsibility and finally full disclosure on the results.

H. Testing

The testing and debugging are done when many Web services encompassed in a system whose qualities and locations are possibly dynamically hosted in several environments with various operating system belong to different retailers and vendors.

IV. CONCLUSION

It has been discussed several security and challenges faced during device-independent Web services and shared some of our experiences in extending to provide the services. The computing based on the web services is currently a technology that is the driver in the software industry and so much productive with respect to the recent, the future needs and requirements in the software industry. It has a lot of benefits in day to day life. It shows in the present scenario, that the power and simplicity of Web services will accelerate innovation in the world of parallel and distribute computing. The existing security practices will not be completely sufficient to cater the security requirements. It can be expected that the emerging technologies issues and its solutions will merge the gap between the services. Also, it will take the operations of the security features to the next level.

REFERENCES

[1] Singhal, Anoop.(2007).Web Services Security: Challenges and Techniques. 8th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY '07), IEEE Computer Society.

[2] Yue, Hua. and Tao, Xu.(2012).Web Services Security Problem in Service-oriented Architecture. International Conference on Applied Physics and Industrial Engineering; Physics Procedia, 24 (2012), 1635 – 1641.

[3] K. N. Gupta , K. N. Agarwala, and P. A. Agarwala. (2005). Digital Signature: Network Security Practices. PHI Pub. New Delhi, ISBN-10: 8120325990, ISBN-13: 978-8120325999.

[4] Chinnici, Roberto., Gudgin, Martin., Moreau, Jean-Jacques., Schlimmer, Jeffrey., and Weerawarana, Sanjiva.(2004). Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language. W3C Working Draft 26-March-2004. https://www.w3.org/TR/2004/WD-wsdl20-20040326/

[5] Gudgin, Martin.(2007). SOAP Version 1.2 Part 1: Messaging Framework (Second Edition). W3C Recommendation. http://www.w3.org/TR/SOAP/

[6] Richard, Robert.(2006).W3C: Universal Description, Discovery, and Integration (UDDI). pp.751-780. DOI: 10.1007/978-1-4302-0139-7_19, http://www.uddi.org

[7] Gutierrez, C., Medina, E. F. and Piattini, M. (2005). Web Services Enterprise Security Architecture: A Case Study. Fairfax. Virginia. USA.

[8] Jiehan Zhou and Eila Niemelä. (2006). Toward Semantic QoS Aware Web Services: Issues, Related Studies and Experience. VTT Technical Research Centre of Finland, Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence (WI 2006 Main Conference Proceedings).

[9] Martino, L. D. and Bertino, E.(2006). Security For Web Services - Standards And Research Issues. Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, IN 47907-2086; CERIAS Tech Report 2006-34.

[10] Mcintosh, M. and Austel, P. (2005). XML Signature Element Wrapping Attacks and Countermeasures. Proceedings of the 2005 workshop on Secure web services (SWS '05), Pages 20-27, Fairfax, VA, USA, November 11 - 11, 2005. ACM, ISBN:1-59593-234-8, doi>10.1145/1103022.1103026

[11] Hal Lockhart.(2005). Security Assertion Markup Language (SAML) 2.0 Technical Overview. Working Draft 03, 20th   February 2005. http://www.oasis-open.org/committees/documents.php?wg_abbre

[12] Ma An-feng and Zhao Feng-yu.(2009). Based on rampart module axis2 Web Service Security Research [J]. Computer Applications and Software, 26 (9): 31-33.

[13] Meng, Wei., Chen, Zhang., Liu, An-huai. and Liu Hailing.(2006). Web Services Security Model and Implementation of Computer Engineering and Applications. Computer Engineering and Applications [J], 2006, 42(26):134-136.

[14] Michael N. H.; Singh, M. P. (2005). Service-Oriented Computing: Key concepts and principles. IEEE Internet computing. 9(1):75-81

[15] Neil. M.O. (2003). Web-Service Security. Tata Mcgraw Hill Pub. New York.

[16] Anne, Anderson., Seth, Proctor. and Godik Simon.(2003). OASIS XACML Profile for Web-services Working Draft 04.

[17] Bellwood, Tom. et. al.(2004). IOASIS UDDI Version 3.0.2 .UDDI Spec Technical Committee Draft, Pp.01-396, Dated 2004- 10-19.

[18] Sinha, Subharta. and Sinha, Smriti Kumar. (2010). Security Issues in Web Services: A Review and Development Approach of Research Agenda. Assam University Journal of Science & Technology: Physical Sciences and Technology Vol. 5 Number II 134-140, 2010.

[19] Aruna. S, .(2016). Security in Web Services- Issues and Challenges . International Journal of Engineering Research & Technology (IJERT), Vol. 5, Issue 09, September-2016. ISSN: 2278-0181

[20] Bartel. Mark., Boyer,John., Fox, Barb., and   Simon. Ed,.(2008). XML-Signature Syntax and Processing (Second Edition). W3C Recommendation 12 February 2008. https://www.w3.org/TR/xmldsig-core/

[21] Kirda. Engin, Kerer. Clemens, Jazayeri. Mehdi. and Kruegel. Christopherl.(2001).Supporting Multi-Device Enabled Web Services: Challenges and Open Problems, Proceedings of Tenth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, (WET ICE 2001), Pp.49-54, 20-22 June.

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)