ISSN : 2231-0711

Julakanti Preetham Kumar et al | International Journal of Computer Science Engineering and Technology(IJCSET) | July 2014 | Vol 4, Issue 7,235-237

A Study on Web Services Security

Julakanti Preetham Kumar[1], Dr Syed Umar[2], Chunduri Sree Harsha[1],Bommareddy Nagasai[1]

[1]*B.Tech Student, ECM dept., K L University, Vaddeswaram, Guntur, AP*

2Assoc.Professor, CSE dept., K L University, Vaddeswaram, Guntur, AP

Abstract. A Web Services have appeared as a new Web-based technology concept for trading information on the Internet using platform-neutral standards, such as XML and adopting Internet-based procedure. In recent times, Web services have initiate vast attractions in both merchants and researchers. It has become a promising technology to design and build complex inter-enterprise business applications. With the increasing number of web services available on the web, the need for web services composition is becoming more and more important. Though, the current Web services architectures are confronted with a few contrary problems. This paper gives an outline and classify the existing Web Services compositions and security.

Keywords: Web Services Composition, Security, Web service Standards

1. INTRODUCTION

A Web Services is quickly rising and a popular standard in applications for sharing data over the web. Several enterprises are working towards using and investing in Web Services in place of their customary client-server computing and in-house servers [1].

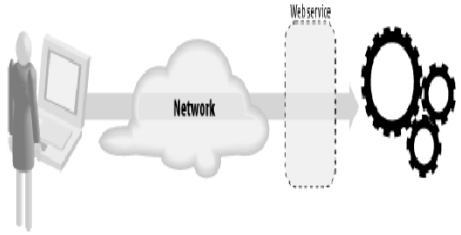

Figure 1. Standard Internet Technologies for web service to allow access application code.

Web service is a network accessible interface to application functionality, built using standard Internet technologies as shown in figure 1.

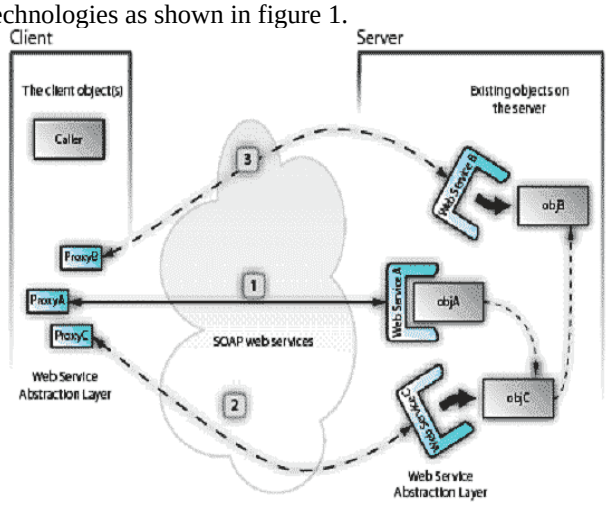

Figure 2. Web Service acts as an abstraction layer.

Web service is an interface positioned between the application code and the user of that code as shown in figure 2. Web service acts as an abstraction layer, separating the platform and programming language specific details of how the application code is actually invoked. Standardized layer means that any language that supports the web service can access the application's functionality. HTML websites today are deployed in web services that we see on the Internet web sites. Application services and the mechanisms for publishing, managing, searching, and retrieving content are access through the use of standard protocols and data formats like HTTP and HTML. The Client applications that understand these standards can interact with the application services to perform tasks like ordering books, sending greeting cards, or reading news. Since the abstraction provided by the standards-based interfaces, it does not matter whether the application services are written in Java and the browser written in C++, or the application services deployed on a UNIX box while the browser is deployed on Windows. Web services allow for cross-platform interoperability in a way that makes the platform irrelevant [2].

2. WEB SERVICES COMPOSITION

Web services composition involves the combination of a number of existing web services to produce a more complex and useful service. The composition of web services is a topic that attracts the interest of researchers. It offers complex problems process ability even with simple existing web services while cooperating with each other. Web service composition is an important technology of SOA that is in a complex and distributed environment and still there are many potential problems [3]. One of main targets of Web service composition is reusing existing web services and composing them into a process. Such programs enable user to manually specify a composition of programs to perform a task, but it is already beyond the human capability to deal with the whole process manually. Despite all efforts, the web service composition still is a highly complex task and generally, the complexity comes from the following sources [4]:

- First, the number of web services available on the Web is increasing dramatically during the recent years and can expect to have a huge repository of web services for searching.
- Second, Web services can be created and updated on the fly, thus the composition systems needs to detect the updating at runtime.
- Third, Web services can be developed by different organizations that use with different concept models for description of the web services. However, not exist

unique language to defining and evaluation the Web services

The variety of composition techniques can be classified according to two approaches. The first is syntactic composition based on syntactic description and other is semantic composition based on semantic description. We will see in this section several approaches for web service composition based on syntactic and web service composition. The overall, the composition of web services can be done in a static or dynamic way. Web service composition contains three methods are: Manual/Static Composition, Automatic/Dynamic Composition, Semiautomatic/dynamic or static Composition. Manual/Static Composition is at syntactic groups. Automatic/Dynamic Composition and Semi-automatic / dynamic / static Composition is at semantic groups. The service composition consists of four different models [5]: workflow-based, artificial intelligence (AI) planning-based, semantic- based, and graph-based.

3. SECURITY

Web services context, security means that the recipient of a message should be able to verify the integrity of the message and to make sure that it has not been modified. WS-Security from OASIS defines the mechanism to include integrity, confidentiality, and single message authentication features within a SOAP message. WS-Security makes use of the XML Signature and XML Encryption specifications and determines how to include digital signatures, message digests, and encrypted data in a SOAP message. WS-Security is concerned with security for SOAP messages, thus, WS Security clearly builds on top of SOAP. In addition, WS Security also makes use of XML Signature and XML Encryption. The Web Services Security (WSS) specifications aim to provide a framework for building secure Web services using SOAP, and consist of a core specification and several additional profiles. The core specification, the Web Services Security: SOAP Message Security specification, defines a security header for use within SOAP messages and defines how this security header can be used to provide confidentiality and integrity to SOAP messages. Confidentiality is provided by utilizing XML Encryption, Integrity of message is provided with the help of the use of XML Signature. While using these mechanisms, message body elements of SOAP, selected headers, or any combination thereof may be signed or encrypted; potentially using different signatures and encryptions for different SOAP roles that because SOAP message headers may be subject to processing and modification by SOAP intermediaries, lower layer security mechanisms such as SSL/TLS are often insufficient to ensure end-to-end integrity and confidentiality for SOAP messages. The functionality of such messages provided by WS-Security is important if confidentiality and integrity are required.

A major performance bottleneck resides in SOAP message processing. The reason for SOAP performance criticality is twofold: On one hand, SOAP communication produces considerable network traffic, and causes higher latency than competing technologies, like Java RMI and CORBA. On the other hand, and perhaps more importantly, the generation and parsing of SOAP messages and their conversion to and from in memory application data can be computationally very expensive.

Whereas the XML encryption does not provides security in these web services yet, and hence an algorithm can be used to provide security to web services. Though, the current Web services architectures are challenged with a few inflexible problems that is, security and the algorithm is used for performing cryptographic operations with symmetric key based security tokens. Existing XML encryption used is symmetric key encryption origin and authenticity of message cannot be guaranteed. Public key encryption allows the use of RSA which enables the recipient of a message to verify that the message is truly from a particular source. The recipient should have received a message confidentially so that unauthorized users could not read it, know the identity of the sender and determine whether or not the center is authorized to carry out the operation requested in the message. These are usually met through encrypting messages. The basic security requirements do not meet as, Security is essential to the approval of Web services by Web services framework and enterprises. Web services require interchange of messages as important issue is to consider when building and using Web services. The application servers are inevitably opened up to application level attacks. Moreover some standards have come out to improve the message security problem, as well as WS Security and various other initiatives towards enabling digital signatures on XML messages and transactions.

The four basic security requirements in Web Services security layer will provide in general as:

1. "Confidentiality" it is the property of information that is not made available or disclosed to illegal individuals, entities, or processes, and guarantees that the contents of the message are not disclosed to unauthorized individuals.
2. "Authorization" means granting of authority, which allows access based on access rights and guarantee that the sender is certified to send a message.
3. " Data integrity" is the property that data has not been undetectably altered or destroyed in an unauthorized manner or by unauthorized users thereby insuring that the message was not modified accidentally or deliberately in transit.
4. "Proof of origin "is evidence identifying the originator of a message or data. It asserts that the message was transmitted by a properly identified sender and is not a replay of a previously transmitted message. This requirement implies data integrity.

3.1 Security Algorithms

Web Service security is big challenge for researchers as it requires a strong security algorithm for the encryption of data. The xml encryption scheme is being used presently for encrypting the messages between the different programming languages running on different platforms, but this xml encryption algorithm is symmetric key encryption algorithm and it creates communication overhead, hence

there is need to use an asymmetric key encryption algorithm.

The more powerful version of DES is used for high security called Triple-DES. In order to start encrypting using Triple-DES, it selects two 56-bit keys. The process of encryption of Data via DES uses three times the key, the first time by the first key, the second time by the second key and the third time by the first key once more. This process creates an encrypted data stream that is unbreakable with today's code-breaking techniques and available computing power, while being compatible with DES. The National Institutes of Standards and Technology considers DES an absolute technology suitable only for legacy applications and today supports a new standard called Advanced Encryption Standard.

AES is a newer encryption standard and is now the preferred one to use for XML Encryption. AES is a substitution-linear transformation network with 10, 12, or 14 rounds, depending on the key sizes, which are currently set at 128, 192, or 256 bits. The block size used in AES is 16 bytes. The data block to be processed is partitioned into an array of bytes forming a matrix with rows and columns. Each cipher operation is byte-oriented.

In symmetric cipher for encryption and decryption it uses the same key. Anyone knowing the key can decrypt all messages encrypted with it, so it needs to be kept secret. In symmetric ciphers Standards DES and AES are the examples. In symmetric ciphers it uses two keys, one for public encryption and the other for private decryption. The advantage is that there's no harm in interface with the public key to anyone, because it can't be used to decrypt anything. As the private key doesn't need to be sent to anyone, and is thus easier to keep secret. In asymmetric cipher RSA is an example. These ciphers are generally much more compute-intensive, so they are rarely used to encrypt large messages [6].

4. CONCLUSION

We have presented Web services, as an rising technology for the Web, The web service overview and the various security issues occurred in the implementation of the xml encryption of the messages. The security of web services is an important aspect and hence a security algorithm is required to implement in web services for key generation and encryption decryption of the messages.

The security algorithm described in this paper will be used together in combination for key generation and encryption decryption of the messages which will provide strong security in web services.

REFERENCES:

[1] R. Sumra, D. Arulazi, "Quality of Service for Web Services-Demystification, Limitations, and Best Practices",March 2003.

[2] Prachi Labhane, Prof. Khushboo Saxena, “Review paper on Web Service Security“, Journal of Advanced Computing and communication technologies , February 2014.

[3] Hu Yan and Wang Hui, "Constraints in Web Services Composition," in IEEE, Dalian, 2008, pp. 1 - 4.

[4] Jinghai Rao and Xiaomeng Su, A Survey of Automated Web Service Composition Methods : Springer Berlin Heidelberg, 2005, vol. 3387.

[5] YU Qing-mei, WANG Lan, and HUANG Dong-mei, "Fishery Web Service Composition Method Based on Ontology," Journal of Integrative Agriculture, vol. 11, no. 5, pp. 792–799, May 2012.

[6] Nils Agne Nordbotten, “XML and Web Services Security Standards”, IEEE Communications Surveys & Tutorials, Vol. 11, No. 3, Third Quarter 2009.