Journal of Theoretical and Applied Information Technology
10th March 2014. Vol. 61 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A FLEXIBLE WEB SERVICE ENVIRONMENT WITH HIGH RANGE OF SECURITY AND QoS MECHANISMS

[1] CHAKARAVARTHI.S , [2] SELVAMANI.K

[1]Research Scholar, Department of Computer Science and Engineering, Anna University, Chennai
[2]Assistant Professor, Department of Computer Science and Engineering, Anna University, Chennai,

E-Mail: [1]chakra2603@gmail.com, [2] smani@cs.annauniv.edu

ABSTRACT

Providing information with Quality of Service (QoS) through Web services is essential to QoS-aware service management and composition. Delivering QoS on the Internet is a critical and significant challenge due to its dynamic and unpredictable nature. Even though the UDDI registry has all the details of WSDL documents provided by the service provider, it does not suggest the client to have a service with QoS parameters. In this proposed model, the UDDI extension is suggest to provide the Quality of Service information the customers. Moreover, the user affords the self encrypted data (privacy preserving) to the requester agent. The requester agent again encrypts the data by providing and considering the important QoS requirement for security. With the process of privacy preserving, the HTTPI protocol having the more secure capability like HTTPs. Thus the property of the HTTPs is integrated with HTTPI protocol and satisfies the QoS requirements for mechanisms, such as authentication, authorization, integrity and confidentiality in various level like Application level, Message Level and Transport level. QoS also covers non functional characteristics like performance (throughput), response time, security, reliability and capacity. This paper also analysis with non functional QoS parameters. Experimental results shows that our proposed work has excellent throughput, good response time and reply size in various configurations.

Keywords: *Quality of Services, UDDI, Web Services, Privacy Preserving*

1. INTRODUCTION

A Web Service (WS) is the technology to swap the self defined messages between two web applications or between two end users. After a great effort for standardization web service applications are discovered and used for execute SOA (Service Oriented Architecture). Web services having various standards defined by W3C and projected by various market giants like Sun Micro Systems, Microsoft, IBM and BEA Systems. In general, WS is a technology to overcome the interoperability problem for an end to end communication over a network. The Web Services standard describes an Extensible Mark up Language (XML) messaging scheme. So that, the end user or the service requester to analyse the exact web application as a web service through the transfer protocol HTTP (Hyper Text Transfer Protocol). The HTTP protocol is very flexible but the security of the protocol is not guaranteed. HTTPS protocol is proposed for security transaction but again getting is more secure and less flexibility. In this paper, the experiments are handled for the analysing the properties of HTTP and HTTPS protocols. In the HTTPI protocol confidentiality is not provided and hence suitable only for social networking and news oriented applications [5]. The set of rules which is used for XML based messaging is known as SOAP. The Web Services Description Language (WSDL) is a XML based application which is used to describe a provision of web service. Web services posted the WSDL document in the registry and the needy (i.e. Service requestor) to analyse the registry and find the appropriate web service. The registry work under the protocol called Universal Description and Discovery Integration (UDDI). It managed all WSDL posts from the web services. If any one of the clients wants to start the transaction with web service, it analyse the UDDI registry and get WSDL document as response which is posted from corresponding web service provider. From the particulars of the WSDL document the client will directly communicate with web service by using the SOAP messaging scheme. By this mode of communication the execution details are completely hide and cannot be seen by any one. After that the client did not require any further details of web service. To overcome the interoperability problems between client and server or provider this model is very useful. The Figure 1 shows the UDDI registry

Journal of Theoretical and Applied Information Technology
10th March 2014. Vol. 61 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and the communication process between service provider and service requestor.

Figure 1 specifies the interaction between the service provider and service requestor, In this UDDI registry has the entire details of the service provider, but still it will not suggest the client for particular service with QoS.

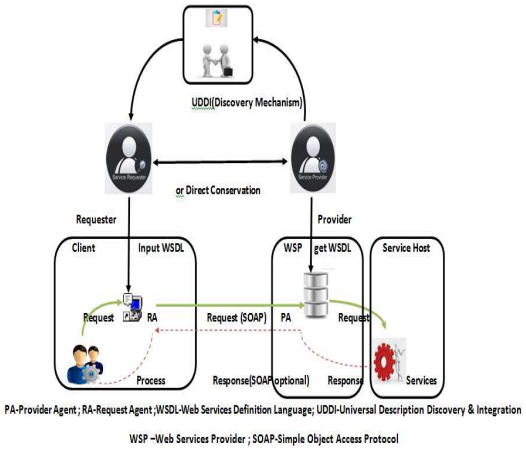

Figure1: UDDI Registry and the Communication Process Between service provider and service requestor

2. RECENT WORKS

NK Prasanna Anjaneyulu Anna proposed his work for an introduction to policy-based security and privacy protection for analyzing several existing policy languages. Also, it shows how these languages can be used in a number of Semantic Web scenarios[1]. Author Jian presented web services security based on water-making techniques through SOAP service. The service suppliers and service recipients are exchanging the information with digital signature and XML encryption technology to secure the message. The way the author has taken to provide security in web services water mark technology [2].

Author Zhuo Hao has proposed remote data integrity checking protocol in a cloud computing for isolated data reliability In addition he has provided feasibility for avoiding third party verification. i.e. un-trusted server for own self verification is provided with reliability [8]. TAO Chun-hua says that Service functions were confused with the concept of QoS, and the functional attributes and non-functional attributes could not be distinguished [3]. Ping Wang discussed the statement, that there is no truly effective extension to the functionality and quality of service. The users 'demand for services had been transformed from a traditional single way for the form of a combination of web services and entity services [4].

3. QOS PARAMETERS FOR WEB SERVICES

3.1 Performance

The performance of web service is an important QoS parameter and is calculated with two aspects namely throughput and latency (response time). The throughput is measured by the equation.

Throughput = No. of Web Services Request / Given Period of Time.

-- -- (1)

3.2 Response Time

The response time is the time between service requester and service provider which is termed as round trip time. The throughput is directionally proportional to QoS rank and latency is in directionally proportional to QoS rank.

Response time = Time taken by client +Time taken by server + time taken by Network + time taken to Load

----- (2)

3.3 Security

The security is very important to all categories especially in web based applications like web services. Even though, there are many benefits from the provider and if we do not provide the security it is more waste. The security of the web services is measured in four categories such as authentication, authorization, integrity and confidentiality. This Paper focus all four categories in our proposed work and analyses the same with QoS parameters. The complete discussion of proposal is in the proposed scheme section.

3.4 Reliability

The main facet among the QoS parameters is the accuracy of the product or an application. To maintain the exact quality always is very important. The reliability of the web service is measured by the no of positive counted in the particular span of time.

Journal of Theoretical and Applied Information Technology
10th March 2014. Vol. 61 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Reliability = No. of Positive Response / Given Period of Time.

------ (3)

3.5 Capacity

The capacity of the service provider or the server is measured by the maximum size of the data replied in the single transaction. Sometimes the provider can reply for more requests if they are having more capacity.

Capacity= Maximum Size of Reply Data / Single Transaction.

----- (4)

4. PROPOSED SCHEME

4.1 An Extension Of Uddi

The UDDI registry doesn't provide any QoS support for the client. It's not necessary when the client need a web service and it will be provide by a single provider but the confusion occurs when the client going to pick a particular requirement which was provided by several providers. To overcome this issue the UDDI shows QoS enabled web services. To attain this data structure of the UDDI registry should be changed as shown in the Fig 2. The example describes in the Fig 2 shows QoS Info which defined as business service sub element.

```
<tModel tModelKey="uuid:1C620754-09E4-4930-AA19-709C62E5210F">
  <name>uudi-org:qosInfo</name>
  <description xml:lang="en">Quality of Service Information</description>
  <overviewDoc>
    <description xml:lang="en"></description>
    <overviewURL>http://www.uddi.org/specification.html</overviewURL>
  </overviewDoc>
  <categoryBag>
    <keyedReference
      keyName="uddi-org:types" keyValue="categorization"
      tModelKey="uddi:1D3FCD00-0DA6-4479-ADFE-B10950C74F62"/>
  </categoryBag>
</tModel>
```

Fig 2: An Extension of UDDI

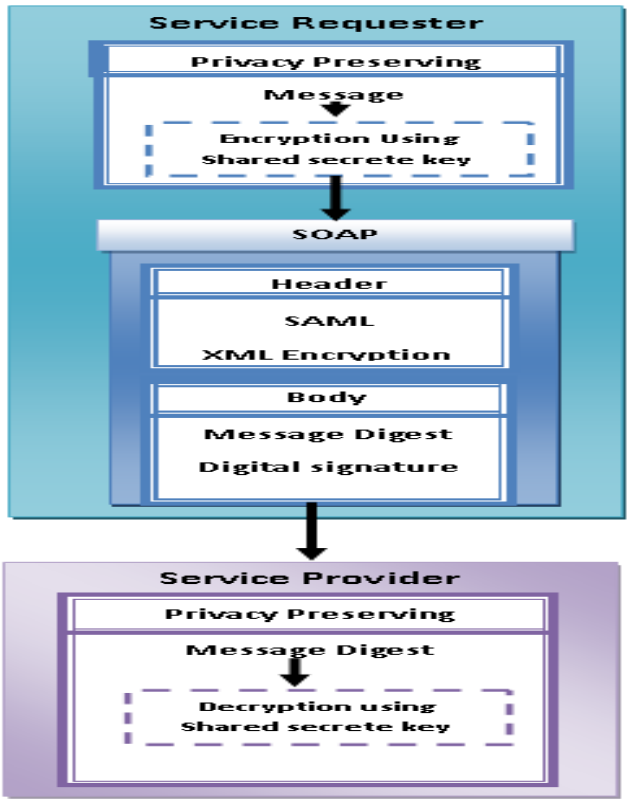

Figure 3 Proposed Web Service Process

4.2 Privacy Preserving

In this proposed model, the user affords the self encrypted data to the requester agent. The requester agent again encrypts the data with QoS requirements for security. With the process of privacy preserving, the HTTPI protocol having the more secure capability like HTTPs.

Thus the property of the HTTPs is integrated with HTTPI protocol and satisfies the QoS requirement of four mechanisms such as authentication, authorization, integrity and confidentiality. In all the three levels such as Application level, Message Level and Transport level security is incorporated. The requester agent sends data from application level to next level i.e. message level; this level is playing superior responsibility in web services in this message level i.e. SOAP message level. The header information can be converted in to binary token form in XML encryption using SAML. The encrypted SOAP is integrated to HTTPi in transport level to keep away from the Man in the Middle (MIM) attack. The proposed web service process is shown in Figure 3.

Journal of Theoretical and Applied Information Technology
10th March 2014. Vol. 61 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. IMPLEMENTATION

Our implementation focus on improving the QoS in web service. The secure web service has been implemented using the asp.Net, c# and WSE3.0.The QoS is achieved by implementing the privacy preserving concept in which the requested message is Encrypted, then the message digest is parameterized to the soap creation this process provides confidentiality, then while creating the soap envelope we add the digital certificate like X509 for the authentication and authorization purpose.

Then the XML encryption take place in which Encryption Extension, Encryption Extension Attribute, Encryption Extension Enum, Encryption Extension Message, Tracing Extension, Tracing Extension Attribute and Tracing Extension Enum sample screen is shown in Figure 4 this feature provides extra security to the data then the envelope created and sends to the web service. In the XML encryption both the request and response are encrypted by tracing it. The implementation of web service method is shown in Figure 5.

The below tables shows that WS scenarios Vs average response time, average throughput and reply size per request and protocols HTTP, HTTPs Vs Response time, reply Size. It's clearly explains combinations of HTTPs and HTTPi provides more secure and most cache accessibility in the WS.

In another experimental setup we maintain the configuration as I3 Processor with 4 GB memory, we conducted the performance test to analyze the HTTP protocol in various browsers such as Internet Explorer, Mozilla Firefox, Google Chrome for throughput (transaction/seconds), average response time (milliseconds) and response size (KB) and the values are tabulated and the results are shown as graph.

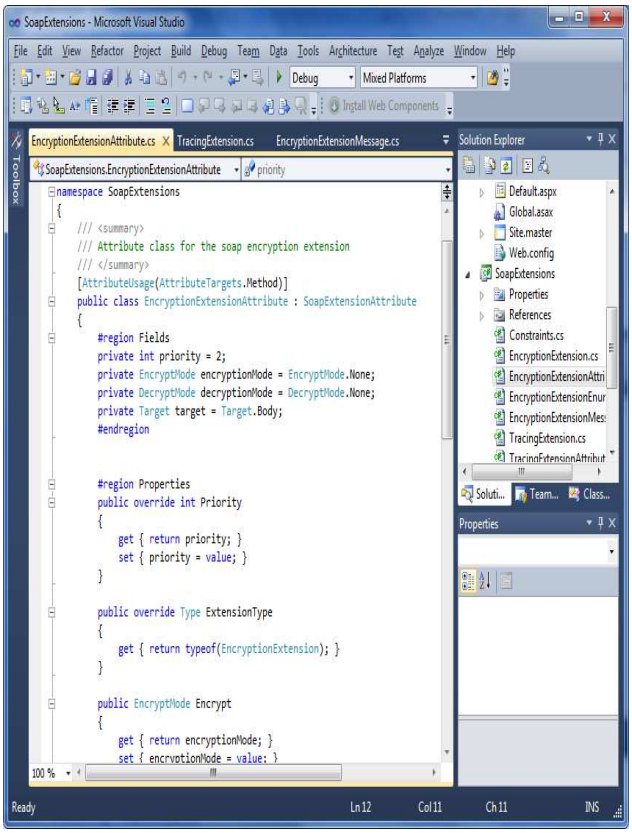

Figure 4: Encryption Extension Attributes

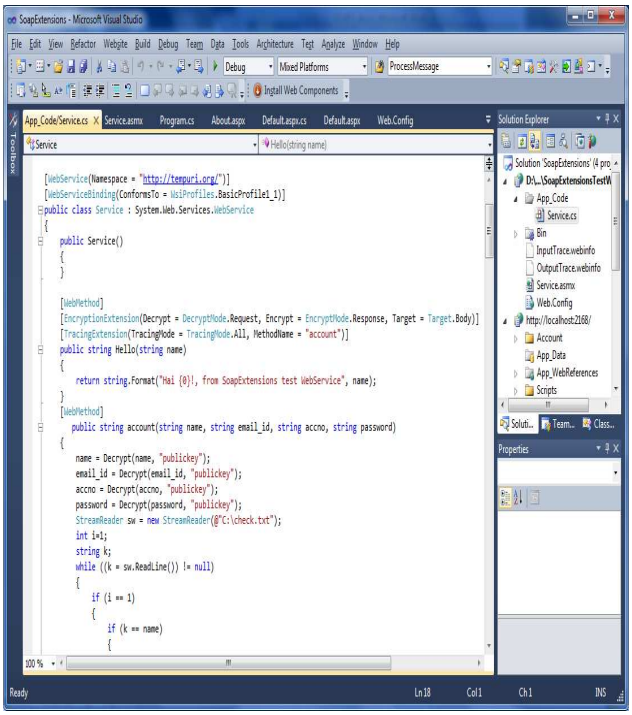

Figure 5: Web Service Implementation

Journal of Theoretical and Applied Information Technology
10th March 2014. Vol. 61 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

6. RESULTS AND ANALYSIS

The web service provider provides the account check, Hello (welcome) service shown in Figure 6 by publishing his web service that can be accessed through the client side.

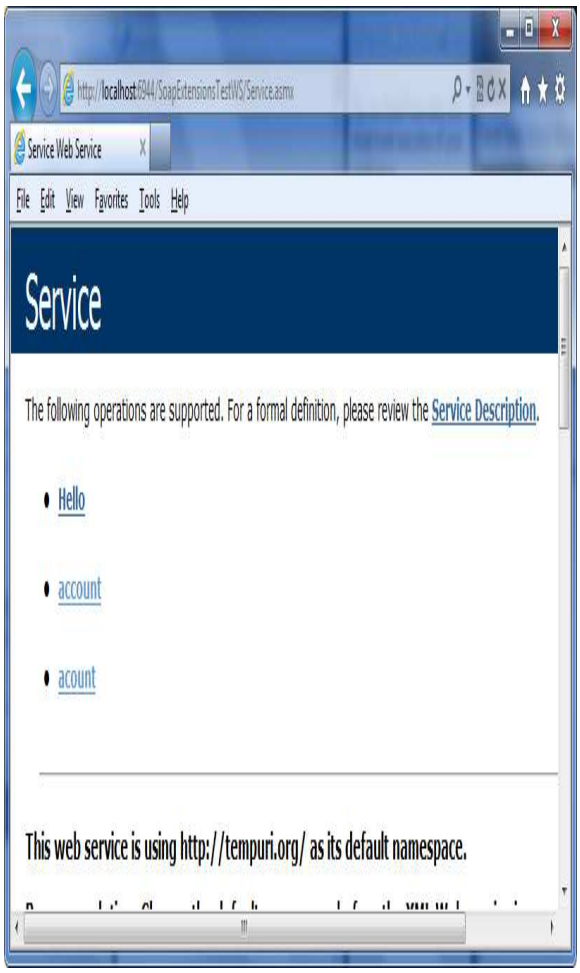

Figure 6: Web Service Provided By Service Provider

The encryption method is implemented in every input, so that even the man in middle attack can be avoided easily. Then in the soap creation the xml encryption and in SAML part Digital signature addition take place which can provide the security, authentication and authorization.

In our experiment we have calculated the response time, reply size and throughput for various browsers which has resulted in different scenarios. Thus for different browsers there will be change in response time, through put and reply size .Table 1 shows the compression of response time of different browsers and are plotted in Figure 7. Table 2 shows the compression of Reply size of different browsers and are plotted in Figure 8. Table 3 shows the compression of throughput between different browsers and are plotted in Figure 9.

Table 1: Comparison of Different Response Time of Http in Different Browsers

Response Time		
Internet Explorer	Fire Fox	Google Chrome
34.2	**33.3**	**26.5**
15.7	**16.3**	**11.6**
15.4	**17.4**	**17.6**
15.6	**17.1**	**16.8**
15.2	**16.8**	**16.5**

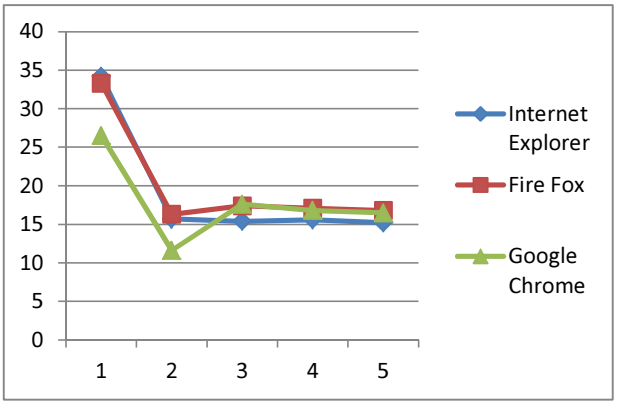

Figure 7: Comparison of different Response time of HTTP in different browsers

From the above graph shown in Figure 7, the response time indicates that our proposed models provides better results with the existing browsers

Table 2: Comparison of Different Reply size of HTTP in Different Browsers

Reply Size		
Internet Explorer	Fire Fox	Google Chrome
12	**12**	**12**

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

10	**10**	**10**
14	**14**	**14**
13	**13**	**13**
15	**15**	**15**

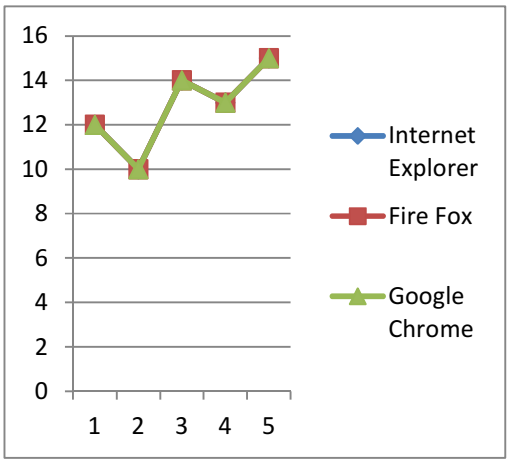

Figure 8: Comparison of Different Reply Size of HTTP in Different Browsers

From the above graph shown in Figure 8, the reply size indicates that our proposed models provides good results with the existing browsers

Table 3: Comparison of Different Through Put of Http in Different Browsers

Throughput		
Internet Explorer	Fire Fox	Google Chrome
6.3	**7.2**	**9.5**
9.6	**9.2**	**15.3**
10.0	**11.5**	**14.2**
9.8	**10.3**	**13.6**
9.5	**9.9**	**13.2**

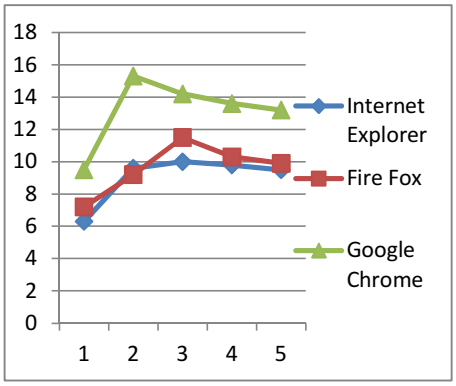

Figure 9: Comparison of Different Throughput of Http in Different Browsers

From the above graph shown in Figure 9, the throughput indicates that our proposed models provides a reasonable in our work with the existing browsers

7. CONCLUSION

The important aspect of end to end business transaction is Quality of Service, which is more important part in web services. The typical QoS mechanisms having various parameters like scalability, robustness, exception handling, accuracy, integrity, accessibility, interoperability, and network-related QoS requirements. QoS also covers non functional characteristics like performance (throughput), response time, security, reliability and capacity. In our paper, we concentrated on all the aspects of QoS like security, reply size, throughput, and response time and. Moreover, we suggest the QoS information in UDDI itself, so that the requesters having flexible environment to select the best web service. With the process of privacy preserving, the HTTPI protocol having the more secure capability like HTTPs. Thus the property of the HTTPs is integrated with HTTPI protocol and satisfied the QoS requirement of four scenarios such as authentication, authorization, integrity and confidentiality in all three levels such as Application level, Message Level and Transport level. The result analysis shows that our experimental results of our proposal having better QoS properties than other.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFERENCES:

[1] N K Prasanna Anjaneyulu Anna and Shaik Nazeer, "Semantic Web Security and Privacy", Journal of Theoretical & Applied Information Technology; 2010, Vol. 22 Issue 1, pp.9-18

[2] Jian Zhang, "A Web Services-based Security Model for Digital Watermarking", Multimedia Technology (ICMT), 2011 International Conference on, 26-28 July 2011.Page:4805 – 4808.

[3] TAO Chun-hua and FENG Zhi-yong, "Novel QoS-aware Web service recommendation model", Application Research of Computers, Vol. 27, No. 10, 2010, pp. 3902-3905,3914.

[4] Ping Wang, Kuo-Ming Cha and, Chi-Chun Lo, "On Optimal Decision for QoS-aware Composite Service Selection", Expert Systems with Applications, Vol. 37, No. 1, 2010, pp. 440-449.

[5] Pankaj Choudhary, Rajendra Aaseri and Nirmal Roberts, "HTTPI based Web Service Security over SOAP", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.3, May 2013, pp. 55-66.

[6] Adam, C., From Web Services to SOA and Everything in Between: The Journey Begins, Webservices.org, May 2005.

[7] Bian WU and Xincai WU, "A QoS-aware Method for Web Services Discovery", Journal of Geographic Information System, 2010, 2, pp. 40-44.

[8] Zhuo Hao, Sheng Zhong and Nenghai Yu, "A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability", IEEE Transactions on Knowledge and Data Engineering, 10 March 2011, Page: 1432 – 1437.