ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

PRIVACY PRESERVING REMOTE DATA TRANSFER IN WEB SERVICE QOS

R.Deepak[1] , M.Mahalakshmi[2] , S.Chakravarthi[3]

P.G. Student, Dept. of Computer Science and Engineering, Saveetha University, Chennai, India[1]

P.G. Student, Dept. of Computer Science and Engineering, Saveetha University, Chennai, India [2]

Associate Professor, Dept. of Computer Science and Engineering, Saveetha University, Chennai, India [3]

ABSTRACT: Remote data integrity checking is a crucial technology in web services. Recently many works focus on providing data dynamics and/or public verifiability to this type of protocols. The goal of the Web Services Activity is to build up a set of technologies in order to direct web services to their complete prospective. Web services are playing excellent role, without web services is not possible to run the www or internet. Day by day the web technologies are improving and it is extended to all the minor or major fields like research, educational, business, etc. Existing protocols can support both features with the help of a third party auditor. This becomes the major disadvantage because third party can misuse our private data. So we develop new mechanism for securing web services, we have to consider five essential areas such as communication level security, communication privacy, zparameter inspection, authentication and authorization. The proposed protocol supports public verifiability without help of a third party auditor. In addition, the proposed protocol does not leak any private information to third party verifiers and also provides security mechanism described above.

Keywords: QOS, Web Service, SOAP, HTTPi

I.INTRODUCTION

Web services are self-described software entities which can be advertised, located, and used across the Internet using a set of standards such as SOAP, WSDL, and UDDI. Web services encapsulate application functionality and information resources, and make them available through programmatic interfaces, as opposed to the interfaces typically provided by traditional Web applications which are intended for manual interactions. A Web Service is a standards-based, language-agnostic software entity that accepts specially formatted requests from other software entities on remote machines via vendor and transport neutral communication protocols producing application specific responses. Web services send and receive data in the form of Extensible Markup Language (XML) messages, which travel via Simple Object Access Protocol (SOAP).

In essence, Web services are like written correspondences; XML serves as the common language in each message and SOAP is the envelope. Despite the technology's growing popularity, security concerns have hobbled some Web services projects. A number of companies have limited their Web services experiments to those within the firewall because of security fears. Quality of service is a combination of several qualities, including availability, security properties, response time, and throughput. Here in this project we focus on security properties.

This process provide authentication, confidentially and integrity to secure the data transfer between one machine to another using token format, XML encryption and XML Signature. For providing the end to end security it follows three

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

types of mechanism. First sign the SOAP message to assure the data integrity it will not provide the non repudiation data. Second Encrypt the SOAP message to assure confidentially. Thirdly to authenticate the data security token maintain in that information. While transferring the information mostly the HTTP based transfer protocol concerned.

It is flexible, lightweight and supported by cache proxies in internet. Using this type of transfer protocol information become less secure and attackers can easily hack the data.

To overcome this problem HTTPS protocol had been implemented to transfer the secure data information which provide three security assurance such as authentication, integrity, confidentiality. Still there is a chance of man in middle attack so we implemented the concept of privacy preserving to avoid it and improve the QOS.

II.LITERTURE SURVEY

M.C. Jaeger, G. Rojec-Goldmann, and G. Mu¨ hl, "QoS Aggregation for Web Service Composition Using Workflow Patterns,"[1] Proc. IEEE Eighth Int'l Enterprise Distributed Object Computing Conf. (EDOC '04), pp. 149-159, 2004. Concept: To determines the QoS of a Web service composition by aggregating the QoS dimensions of the individual services. To verify whether a set of services selected for composition satisfies the QoS requirements for the whole composition.The aggregation performed builds upon abstract composition patterns. Algorithm: Aggregation algorithm, Recursive approach. Merits:Some classification is not beneficial for aggregation because Some QoS dimensions are not numerical values, which can be mathematically aggregated. Demerits:Its not evaluate the contributions of modelling workflows or compositions of Web Services with Petri Nets. [2]G. Canfora, M.D. Penta, R. Esposito, and M.L. Villani, "QoSAware Replanning of Composite Web Services," Proc. IEEE Int'l Conf. Web Services (ICWS), pp. 121-129, 2005. Concept: QoS-aware composition using a monitoring mechanism. QoS values changes could increase the risk of breaking SLAs and obtaining a poor QoS. So to use triggering algorithm composite service replanning during execution. Demerits: Run-time service discovery and late-bindingMerits: Early activation of the replanning, so to prevent risks as soon as possible Algorithm Used:Triggering algorithm. J. Cardoso, J. Miller, A. Sheth, and J. Arnold, [3]"Quality of Service for Workflows and Web Service Processes," J. Web Semantics, Concept: The predictive QoS model that makes it possible to compute the quality of service for workflows automatically based on atomic task QoS attributes. We also present the implementation of our QoS model for the METEOR workflow system. Algorithm Used: SWR algorithm Merits QoS-based design. QoS-based selection and execution. QoS monitoring. Demerits: To predict and analyse the QOS is difficult. H. Zheng, W. Zhao, J. Yang, and A. Bouguettaya, "QoS Analysis for Web Service Composition," [4] Proc. IEEE Int'l Conf. Services Computing (SCC '09), pp. 235-242, 2009. Concept: To calculate the QoS for composite services with complex structures. Based on the proposed QoS calculation method. Merits calculate QoS for composite services with arbitrarily combined patterns. Demerits : It will not calculate the different service selection methods. Algorithm Used: QOS calculation.

II. OBJECTIVE

The Objective of our project is to improve the quality of service in the security aspect by providing the privacy preserving technique and also provide authentication, integrity, and confidentiality.

III. EXISTING SYSTEM

The data transferred in the web service is so important that the clients must ensure it is not lost or corrupted. The client transfers his data in the server without keeping a local copy.

ISSN: 2319-8753

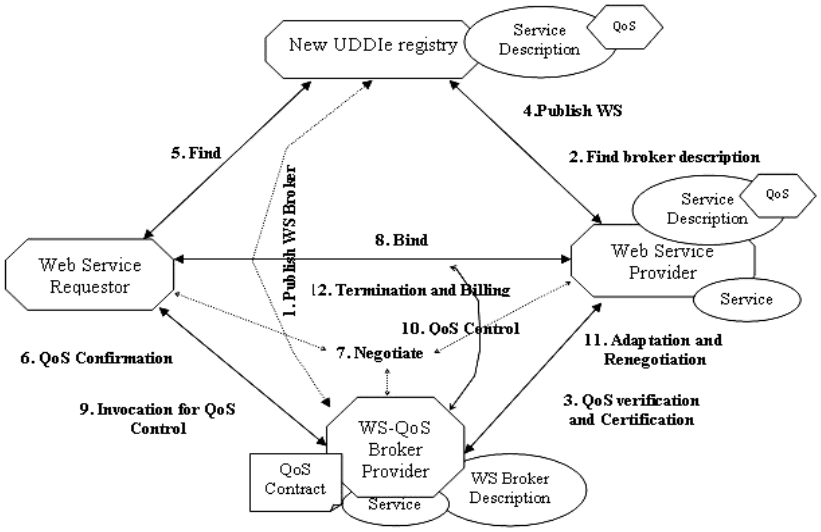
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

Hence, it is of critical importance that the client should be able to verify the integrity of the data transferred/stored in the remote entrusted server. If the server modifies any part of the client's data, the client can't be able to detect it.

Web service users have to go for third party for security reason who may leak our information without any trace.



IV. PROPOSED SYSTEM

1. The proposed protocol inherits the support of data dynamics from , and supports public verifiability and privacy against third party verifiers, while at the same time it doesn't need to use a third-party auditor.

2. We give a security analysis of the proposed protocol, which shows that it is secure against the untrusted server and private against third party verifiers.

3. The proposed mechanism also provides communication level security, communication privacy, parameter inspection, authentication and authorization.

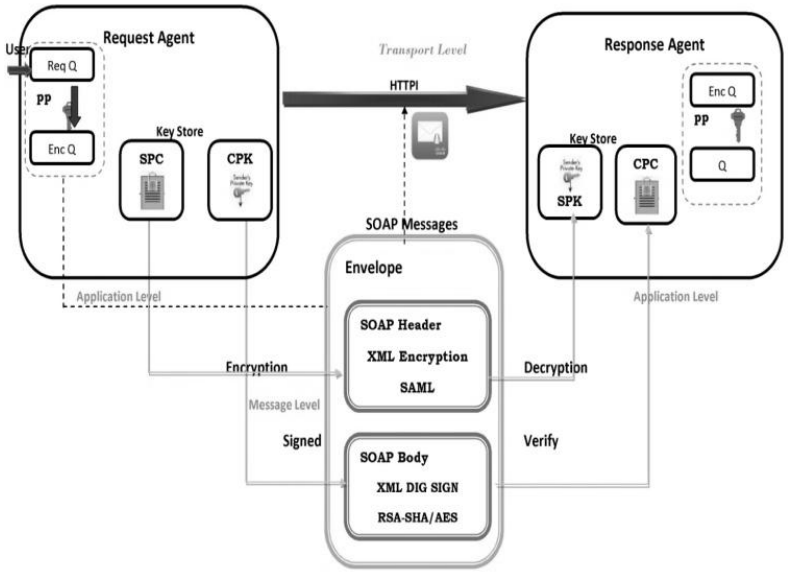
ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

4.1 Proposed System Architecture



V. MODULAR DESCRIPTIONS

5.1 Web service creation

A web service is a web application which is basically a class consisting of methods that could be used by other applications. It also follows code-behind architecture like the ASP.Net web pages, although it does not have a user interface. To understand the concept let us create a web service that will provide online bank transaction. The clients can query about the balance and also deposit and withdraw the amount based on his or her username and password. Here the web page is designed separately and other process is developed separately in web service then the web reference is added to the required web site to join both web page and web service.

5.2 Privacy Preserving

Privacy preserving is a concept in which ideal-model adversary cannot learn more about the honest party's input than what is revealed by the function output. Here in this module we implement privacy preserving using cryptographic concept like Des encryption and decryption to hide the user input from man in middle attack and provide confidentiality.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

5.3 Xml Security

The XML security is provided by the soap protocol in which the XML encryption takes place. XML Encryption uses the Key Info element, which appears as the child of a Encrypted Data, or Encrypted Key element and provides information to a recipient about what keying material to use in decrypting encrypted data. The Key Info element is optional: it can be attached in the message, or be delivered through a secure channel like HTTPS.

5.4 X509 Authentications

In the X.509 system, a certification authority issues a certificate binding a public key to a particular distinguished name, or to an alternative name such as a unique-id, e-mail address or a DNS entry. Here we add X.509 certificate with our transaction data for authentication and authorization process.

5.5 Envelope creation and Transaction

Here in this module SOAP envelope is created by joining the user data, xml security and X509 certificate and form the soap with authentication, authorization, confidentiality thus our xml data is transmitted with secure environment.

VI. RESULT AND DISCUSSION

The proposed protocol is suitable for providing integrity protection of customers' important data. The proposed protocol supports data integrity, confidentiality, authentication and authorization at the block level, and also supports public verifiability. The proposed protocol is proved to be secure against an entrusted server. It is also private against third party verifiers. Both theoretical analysis and experimental results demonstrate that the proposed protocol has very good efficiency in the aspects of communication, computation, authentication and storage costs. There will be no other security mechanism needed because the four parameters of security data integrity, confidentiality, authentication and authorization achieved in this protocol itself.

VI. CONCLUSION

In this paper I propose a new remote data transfer in web services with QOS. The proposed protocol is suitable for providing integrity protection of customers' important data. The proposed protocol supports data insertion, modification and deletion at the block level, and also supports public verifiability. The proposed protocol is proved to be secure against an untrusted server. It is also private against third party verifiers. Both theoretical analysis and experimental results demonstrate that the proposed protocol has very good efficiency in the aspects of communication, computation and security. The difficulty is that there is no clear mapping relationship between the data and the tags. In the current construction, data level dynamics can be supported by using block level dynamics.

Future works includes extending the approach to other domains. It would also be very interesting to deal with more complex applications depending on the attacks that affect both the web and other application. Whenever a piece of data is modified, the corresponding blocks and tags are updated. However, this can bring unnecessary computation and communication costs. We aim to achieve data level dynamics at minimal costs in our future work.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

REFERENCES

[1] M.C. Jaeger, G. Rojec-Goldmann, and G. Mu¨ hl, "QoS Aggregation for Web Service Composition Using Workflow Patterns," Proc. IEEE Eighth Int'l Enterprise Distributed Object Computing Conf. (EDOC '04), pp. 149-159, 2004.
[2] G. Canfora, M.D. Penta, R. Esposito, and M.L. Villani, "QoSAwareReplanning of Composite Web Services," Proc. IEEE Int'l Conf. Web Services (ICWS), pp. 121-129, 2005.
[3] J. Cardoso, J. Miller, A. Sheth, and J. Arnold, "Quality of Service for Workflows and Web Service Processes," J. Web Semantics, vol. 1, pp. 281-308, 2004.
[4] H. Zheng, W. Zhao, J. Yang, and A. Bouguettaya, "QoS Analysis for Web Service Composition," Proc. IEEE Int'l Conf. Services Computing (SCC '09), pp. 235-242, 2009.
[5] M. Dumas, L. Garcı´a-Ban˜ uelos, A. Polyvyanyy, Y. Yang, and L. Zhang, "Aggregate Quality of Service Computation for Composite Services," Proc. Int'l Conf. Service Oriented Computing (ICSOC '10), pp. 213-227, 2010.
[6]L. Zeng, B. Benatallah, A. Ngu, M. Dumas, J. Kalagnanam, and H. Chang, "QoS-Aware Middleware for Web Services Composition," IEEE Trans. Software Eng., vol. 30, no. 5, pp. 311-327, May 2004.
[7] Q. Yu and A. Bouguettaya, "Framework for Web Service Query Algebra and Optimization," ACM Trans. Web, vol. 2, no. 1, pp. 1-35, 2008.
[8] L. Zeng, B. Benatallah, A. Ngu, M. Dumas, J. Kalagnanam, and H. Chang, "QoS-Aware Middleware for Web Services Composition,"IEEE Trans. Software Eng., vol. 30, no. 5, pp. 311-327, May 2004.
[9] Q. Yu and A. Bouguettaya, "Framework for Web Service Query Algebra and Optimization," ACM Trans. Web, vol. 2, no. 1, pp. 1-35, 2008.
[10] H. Zheng, W. Zhao, J. Yang, and A. Bouguettaya, "QoS Analysis for Web Service Composition," Proc. IEEE Int'l Conf. Services Computing (SCC '09), pp. 235-242, 2009.
[11] M. Keidl and A. Kemper, "Towards Context-Aware Adaptable Web Services," Proc. 13th Int'l World Wide Web Conf., pp. 55-65, May 2004.
[12] A. Abraham, J. Chung, and S. Han, "Web Services: Recent Advances and Applications," J. Digital Information Management, vol. 4, no. 1, pp. 1-3, 2006.
[13] F. Gandon and N. Sadeh, "Semantic Web Technologies to Reconcile Privacy and Context Awareness," Web Semantics: Science, Services and Agents on the World Wide Web, vol. 1, no. 3, pp. 241-260, 2004.
[14] H. Truong and S. Dustdar, "A Survey on Context-Aware Web Service Systems," Int'l J. Web Information Systems, vol. 5, no. 1, pp. 5-31, 2009.
[15] L. Li, D. Liu, and A. Bouguettaya, "Semantic Based Aspect- Oriented Programming for Context-Aware Web Service Composition," Information Systems, vol. 36, no. 3, pp. 551-564, 2011.