Indian Journal of Science and Technology, Vol 9(37), DOI: 10.17485/ijst/2016/v9i37/102084, October 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Enhancing Data Privacy in Web service Composition

R. Mangalagowri* and B. Muruganantham

Department of Computer Science, SRM University, Chennai - 603203, Tamil Nadu, India;
mangalagowri.r@ktr.srmuniv.ac.in, muruganantham.b@ktr.srmuniv.ac.in

Abstract

Background/Objectives: Various types of web services are offered on the internet, which led to increasing the interest in the area of web service composition by utilizing many available web services. Web services will be acting like as interface for providing cross-organizational collaborations on the internet. **Methods:** To ensure the privacy of consumer data in cross-organizational composition services where, no proper collection, maintenance and delivery of the sensitive data is available. A framework has been proposed in this paper that addresses consumer privacy concerns in composite web services. This framework provides a technique for privacy policy checking between a user and a service provider for compatible privacy policies. **Findings:** Web services composition environment are highly computerized, vibrant, and diverse in nature. These attributes provide the high level of risk on the communication entities on the internet. **Applications:** The structure applies to the Hospital Management System, Which involves three entities called a patient, consultant and service providers. The encryption and multi-level of authentication ensure the Privacy of the sensitive data.

Keywords: Discovery and Integration, Multi-level authentication, Simple Object Access Protocol, Universal Description, Web Services Description Language

1. Introduction

The Internet can access the Web service, through an Application Programming Interface, which offers various functionalities. Web services are self-explanatory, modular applications, which can be registered, published and invoked by end users across internet[1,2]. Web services are designed to perform tasks, which ranges from simple to complex tasks. Web services are used to expose the functions onto the network. It provides low communication cost, loosely coupled applications and used to connect different applications. Web services use XML language for structuring the data and SOAP protocol for data transfer over the internet. It uses Web Services Description Language (WSDL)[3], Universal Description, Discovery and Integration (UDDI), and SPARQL.A large number of Web services are developed and delivered on the internet. Consumer needs can be satisfied by single web service or combination of various web services despite their development environment and implementation technologies[4,5].

In Transferring our sensitive information without the administrator control may increase the danger of allowing potential attackers to collect, disclose sensitive data in detrimental ways. In proposed A QoS model4 which calculates a seclusion risk of published sensitive data. The major hand-outs of this paper includes calculating a privacy threat of disclosed sensitive data, delivering Web service composition with privacy defend and QoS assertion. In proposed A framework[6] to handle security in web services compositions and using WS-Security and WS-Policy[7]. The main parts of this framework are the aspect-based process container, the security service, and the deployment descriptor. In the Existing System, a Model was developed to unfold Data providing (DP) Services and service oriented queries. DP Services have mapped as RDF views over Mediated Ontology. Semantic relationship between input and output parameters are assigned using this RDF view. Query rewriting algorithm was developed to process the queries. Query Mediator converts input query into the composition of web services.

*Author for correspondence

Composing new web services from already available web services to provide new functionality to satisfy customer ad business needs has introduced privacy issues. To overcome privacy breaches, a newly developed framework is addressing consumer privacy concerns in composite web services.

2. Proposed Framework

In proposed framework provides a technique for privacy policy checking between an end user and a service provider for compatible privacy policies. It is used to enhance the privacy when the user is requesting for the services. Privacy of the user is checked before they are seeking for some service. Various levels of preferences can test the privacy. When the user satisfies the privacy policies, he is allowed to give their request in natural language. Those requirements convert into SQL queries. The Composition of various web services will answer these service requests. The following Figure 1 shows overall architecture of the proposed framework. The concept applies to the Hospital Management System, which involves three entities called Patient, Consultant, and Service Provider. Privacy of the Patient, Consultant and Service Provider data are enhanced using encryption, multi-level authentication and randomly generated security questions. The proposed framework involves following four phases called Registration Module, Patient Module, Consultant Module and Service Provider Module.

2.1 The Registration Module

This module allows the new user to register for accessing the application and allow the existing user to login inside the application. To login in the application, The Main page is created. It includes two options 1) new user, 2) Existing user as shown in Figure 2. Whenever clicking on the new user it provides the following options like Patient Registration, Consultant Registration and Service Provider Registration where each entity has to enter the required details along with they has to answer the secret questions listed on the page. To enhance the privacy sensitive information are stored in an encrypted format using SSL encryption algorithm. In case of existing user Patient, Consultant and Service Provider has to enter the username, Password, Secret Question and Answer for the secret question correctly. If the above entities are giving wrong details after the second time also, then they are blocked from accessing his page.

2.2 The Patient Module

The patient module allows the patient to perform following functionalities. 1. Updating the Patient Details, 2. The Addition of Medical History, 3. Viewing the Analysis Report, 4. Viewing Consultant details, 5. Generation of Bill as shown in Figure 3.

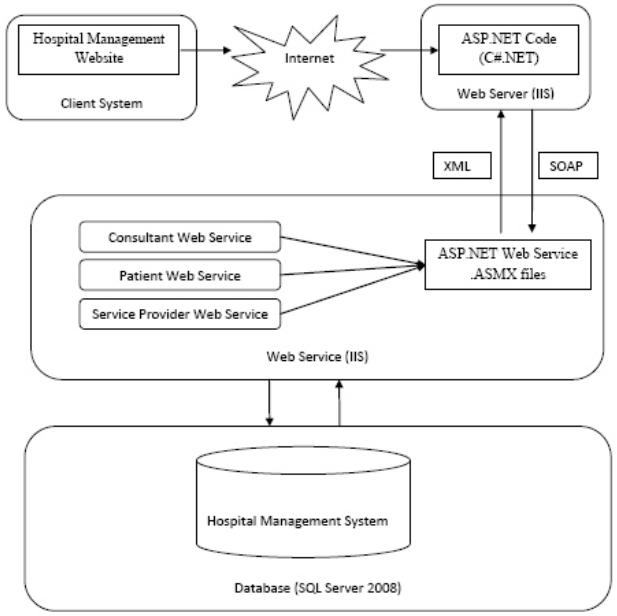

Figure 1. Architecture of the Proposed System.

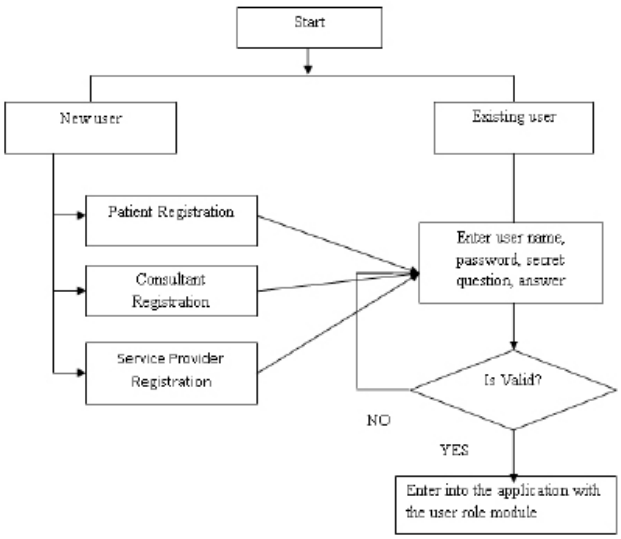

Figure 2. Registration Module.

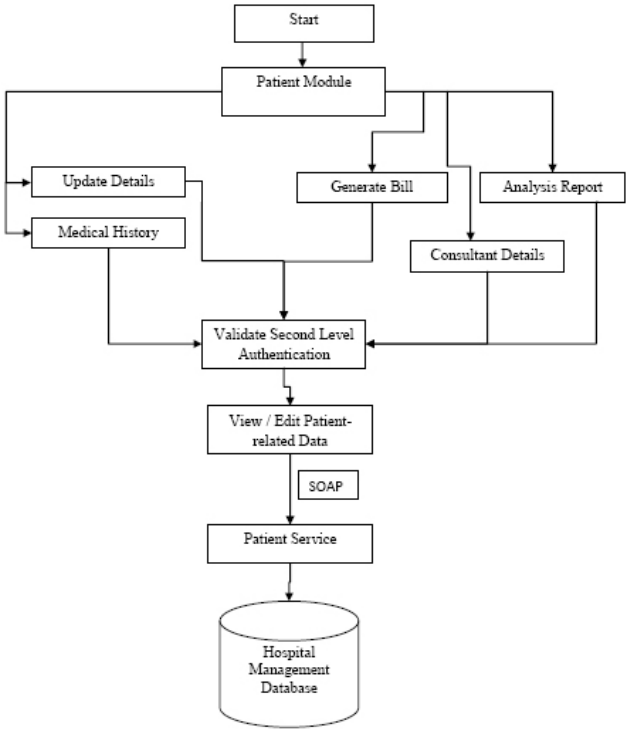

Figure 3. The Patient Module.

2.2.1 *Second Level of Authentication*

Authorized access to the patient is checked again by the administrator by answering the second tier of secret questions, which provides the flexibility to answer one set of questions. Once the patient is authorized he can access this page which includes the functionalities as mentioned above like the patient is allowed to update his details, he can add the following details like Type of disease, Consultant name, Consultant Id, Date of consultation and Medicine prescribed in his medical history. The patient is authorized to access the Consultant details by specifying the specialization of the Consultant; he is allowed to see the analysis report provided by the consultant and the bill generated.

2.3 The Consultant Module

The Consultant module allows the consultant to perform following functionalities. 1. Updating the Consultant Details, 2. Viewing Appointment Details, 3. Updating Diagnosis Result and 4. Preparing Analysis Report as shown in Figure 4. Once the consultant is authorized he is allowed to update his profile, Consultant can view the Patient details by specifying the Date of Appointment.

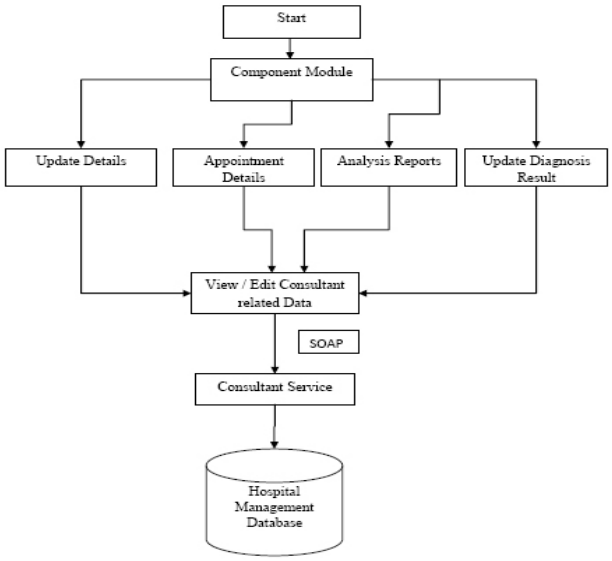

Figure 4. Consultant Module.

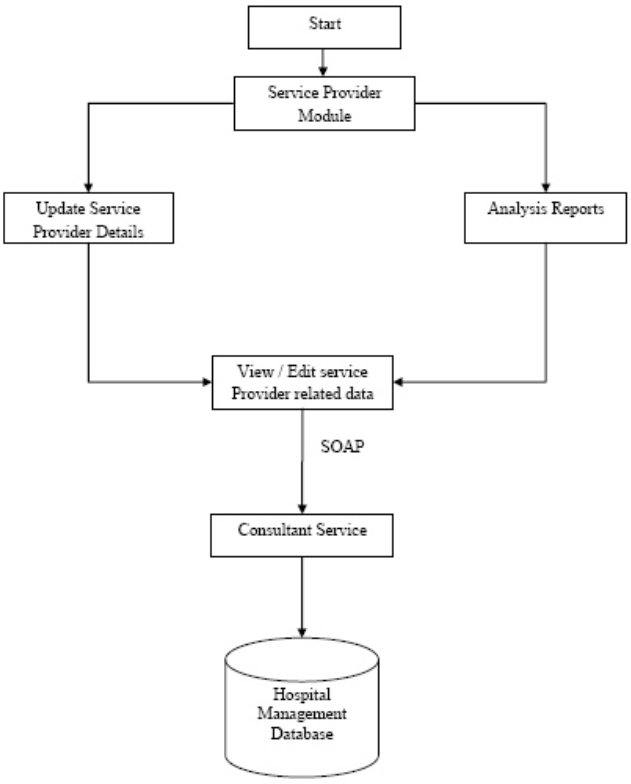

Figure 5. Service Provider Module.

The Consultant can select particular Patient and see his medical history and he can prepare the analysis report based on the diagnosis result.

2.4 Service Provider Module

This Module allows the Service Provider to perform following functionalities. 1. Updating the Service provider details, 2. Analysis Report as shown in Figure 5. Once the Service Provider is authorized he is allowed to update his profile, generate Analysis Report based on IN and OUT Patients.

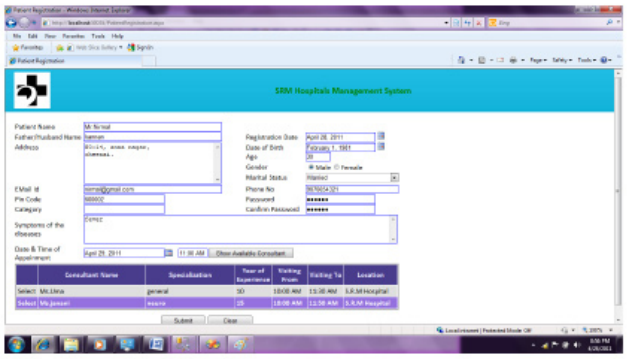

Figure 6. Patient Registration Page.

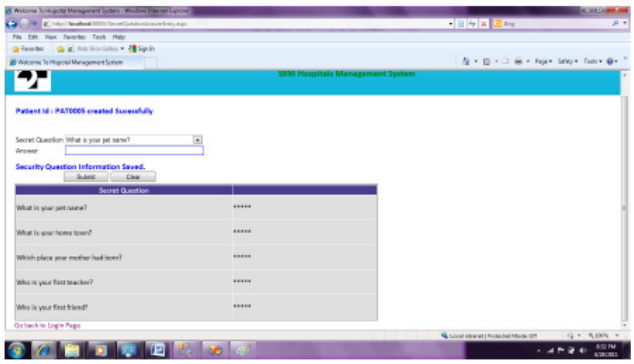

Figure 7. Secret Question Page.

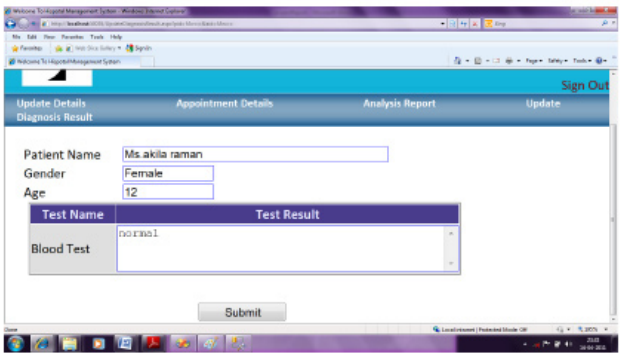

Figure 8. Diagnosis Result.

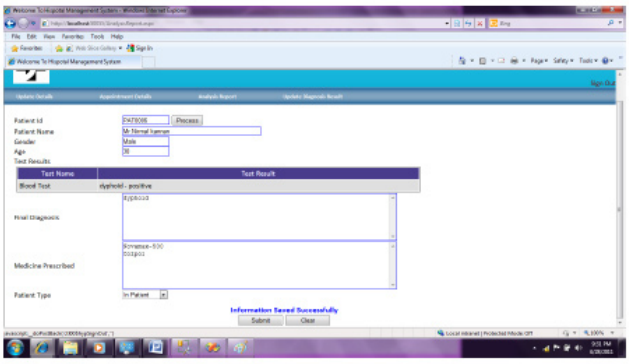

Figure 9. Analysis Report.

3. Result Pages

The proposed framework is implemented using C#, ASP.Net technologies. Asp.Net web services are created for each functionality done in the registration module, patient module, consultant module and service provider modules. The snapshots of various feature shown in the Following Figure 6 to Figure 9.

4. Conclusion

The proposed framework enables the privacy of patient, consultant, and service provider data by encrypting sensitive data of the patient, consultant and service provider in the Hospital Management system. Each user has to answer for a set of secret questions Apart from username and password. The secret questions generated randomly each time the user is logging into the application. If the user is answering wrong after second time also means he cannot access the particular page. Multi-level authentication avoids unauthorized access to sensitive information. As a future work Quality of Service (QoS) will be considered while processing queries and composing the services. The Service Provider module can be extended to perform various types of analysis like Consultant based analysis and Diseases based analysis. The Patient Module can be extended to send mail to the service provider when the patient cannot access.

5. References

1. Liu L, Huang Z, Xiao F, Shen G, Zhu H. Verification of Privacy Requirements in Web Services Composition. Second International Symposium on Data Privacy and E-Commerce. 2010 Sep; 117–22.

2. Liu K, Wang Q, Han J, Wu H. A Privacy Protection Method for P2P-based Web Service Discovery. IEEE International Conference on e-Business Engineering. 2007 Oct. p. 551–8.
3. Suchithra M, Ramakrishnan M. A Survey on different web service discovery techniques. Indian Journal of Science and Technology. 2016 Mar; 9(11):1–10.
4. Yu T, Zhang Y, Lin K-J. Modeling and Measuring Privacy Risks in QoS Web Services. IEEE International Conference on Enterprise Computing E-Commerce and E-Services. 2006 Jun. p. 1–4.
5. Amudhavel J, Prabu U, Inbavalli R, Moganarangan N, Ravishankar V, Baskaran R, Dhavachelvan P. Survey and Analysis of web service Composition Strategies: A state of art performance study. Indian Journal of Science and Technology. 2016 Mar; 9(11):1–10.
6. Charfi A, Mezini M. Using Aspects for Security Engineering of Web Service Compositions. IEEE International Conference on web services. 2005 Jul; 1:59–66.
7. Jensen M, Gruschka N. Privacy against the business partner: Issues for realizing end-to-end confidentiality in web service compositions. The 20th International Workshop on Database and Expert Systems Application. 2009 Oct; 117–21.