ISSN 2319 – 7595
Volume 5, No.1, January – February 2016
International Journal of Information Systems and Computer Sciences
Available Online at http://warse.org/IJISCS/static/pdf/file/ijiscs02512016.pdf

A Privacy Based Approach in DaaS for Secure Data Accessibility

SYED HYDER[1], G.MINNI[2], SAYEED YASIN[3]
[1]M.Tech CSE Student, Nimra Engineering College Vijayawada Andhra Pradesh, India
[2]Assistant Professor, Dept of CSE, Nimra Engineering College Vijayawada Andhra Pradesh, India
[3]Associate Professor, HOD of CSE, Nimra Engineering College Vijayawada Andhra Pradesh, India

ABSTRACT

Web service composition is a network technology with the aim of merging information commencing from more than one resource into a single web application. Web services are platform independent and language independent. Data as a Service (DaaS) builds on service-oriented technologies to enable fast access to data resources on the Web. The composition of Daas (Data-as-a-service) services is a powerful solution for binding value-added applications on top of existing ones. However, this paradigm raises several new privacy concerns that traditional privacy models do not handle. The revealing of privacy sensitive information is one of the key challenging issues in Daas composition. Protecting privacy of online users in social networks can be done using dynamic approach for enhancing privacy in web service composition. The data from multiple sources can be integrated which can rise many problems in one by simply joining multiple data sets would reveal privacy sensitive information. The personal privacy sensitive information can be revealed.

Key words: Daas- Data as a Service.

1. INTRODUCTION

Modern ventures across all scales are moving towards a service-oriented architecture by putting their information behind the web services by providing a platform independent method for interacting with their data. A web service is defined as a software function which is provided over the web or a cloud at a network address. It is defined as a service that is “always on”. Now-a-days web services are emerged as a accepted medium for data distributing and allocating on the web. In epidemiological researches there is need for data sharing which is obvious for making better health environment of people. They should consider multiple data sources such as patient disease, social conditions and his geographical factors. The Daas services provides the data sources and they are organized with peers. The web service source defines the input message of a web service operation and represents the metadata for a web service SOAP request.P2p is an alternative network model provided by traditional client server architecture. It uses a decentralised model in which each machine is defined as a peer, functions as a client with its own layer of server functionality.DaaS [3],[6] is a cousin of software as a service. Daas is based on the concept that the data can be provided on demand to the users regardless of their geographic or organizational separation of provider and user. In this the information is stored in cloud and is accessible by a wide range of systems and devices. DaaS is a distribution and information provision model in which data files such as text, images and videos are available to customers over the internet. The scope of Dynamic approach for Enhancing Privacy in Web Service Composition is spread around the world where the web services are used. It is used in the medical field, online applications and many services where internet is used for sharing the data.

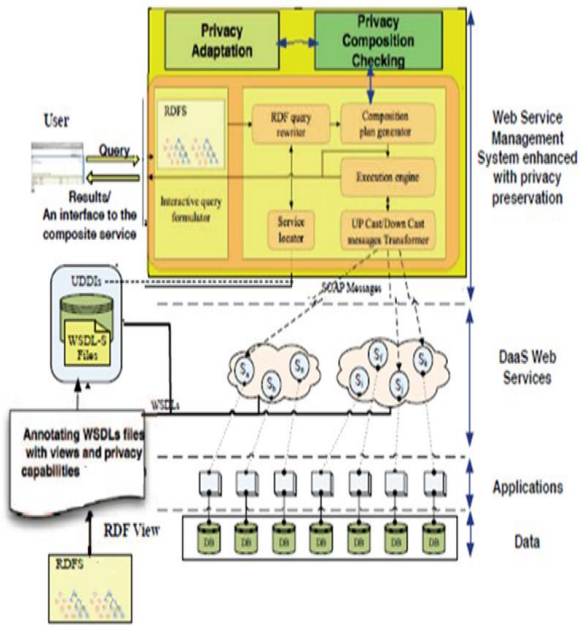
2. RELATED WORK

In this work [5] they discuss the issues related to web services and they discover a new web service model. Web services technology became popular in many areas because of its potential. It provides a guarantee solution for addressing platform interoperability problems which are faced by the system integrators. It is a regulated model that can co-exist with the de-regulated UDDI registers. It differs from the current UDDI model by having information about the functional explanation of web service as well as its quality of service is registered repository. The web service provider offers web service by publishing the service into the registry. The web service consumer needs the web service offered by the provider. The UDDI register is the repository of registered web services. The web service QoS certifier verifies the claims of quality of service for a web service before its registration. Web Services are powered by four core technologies. They are XML, WSDL, UDDI, SOAP. Before building a web service, developers create its definition in the form of WSDL document which describes the service’s location and functionality of service provider on the web. Information about a service is entered into a UDDI register, which allows consumer to search for and locate the services they need. Using the information present in the UDDI register the developer uses the instructions in WSDL to construct SOAP messages for exchanging data with the service over HTTP.

3. METHODOLOGY

After surveying the papers the problem is defined as, the emergence of analysis tools makes it easier to analyze and combines more amount of information, there increases the risk of privacy violation. Many privacy challenges arise during the service composition. Generally privacy is defined as the right of an entity to define to what extent the information is provided to the user. The proposed system Daas enables data access on demand to user regardless of any location. But it lacks mainly in two factors they are Daas collects and stores huge amount of user's information. These services are able to share this information with other services. The privacy challenges that arise during service composition are there is a need for a proper privacy model to define and specify the private data. Any two web service that participates in a composition may require the same input data that is not disclosed by the other service because of privacy concerns. The main drawback in service compositions is dealing with the incompatible privacy policies.

The dynamic approach for enhancing privacy during web service composition system enhances the privacy during a web service composition. The privacy challenge that arises during web service composition is reduced. It eliminates the incompatible privacy policies during service composition. The user provides a keyword query against an RDF query and it looks for all the sub-graphs which contain the keyword. The data generated in RDF format is converted into RDF triple which is in one line of a file. The query processing is done using SPARQL queries. The efficient data can be retrieved from different web services using SPARQL queries. Therefore the privacy of data is enhanced during a web service composition.



4. IMPLEMENTATION DETAILS & PROGRAM DESIGN

In this application Dynamic approach For Enhancing Privacy in Web Service Composition, we implement the data by using various web services. These services may include services providing information about buses, their routing allocation services, booking services, and ch other search details about drivers and routes. Here we store all the information about the buses and other details in RDF files. To know all the details about buses first we have to sign up in this application. The members have to enroll their details. Through their details only, they can login into the application and can check for the information. If there is no data available it stores the data in the database. Using the login name and password the user can login into the application. The administrator can enter the details into the database and update the details about buses, drivers and routes. The user can check only details about the buses. Thus the project is implemented by using the users and the administrator.

Here we use different technologies for the implementation of this project. We use HTML to see the information of the content. Java technology is used for the running of the project. Here we use the HiedSQL for the storage of the data that is entered by the user. The server we are using to run the project is the Apache Tomcat Server. Java Servlet pages are used to link project with the dynamic pages. The database tables that are used in this application are described in the SPARQL language.

A. Data Generation and storage

Intuitively, a keyword query against an RDF graph looks for (smallest) sub-graphs that contain all the keywords. Given an RDF graph G = {V,E}, for any vertex v∈V, denote the keyword stored in v as w(v). For the ease of presentation, it is assumed each vertex contains a single keyword. The data generated in RDF serialization format. Therefore we convert the data to N-Triples to store the data, because with that format we have a complete RDF triple (Subject, Predicate and Object) in one line of a file.

B. Triples

An RDF dataset is a graph (RDF graph) composed by triples, where a triple is formed by subject, predicate and object in that order. When such ordering is important semantically, a triple is regarded as a directed edge (the predicate) connecting two vertices (from subject to object). Thus, an RDF dataset can be alternatively viewed as a directed graph. W3C has provided a set of unified vocabularies (as part of the RDF standard) to encode the rich semantics. From these, the rdfs:type predicate (or type for short) is particularly useful, since it provides a classification of vertices of an RDF graph.

C. **Pre-processing**

The summarization process starts with splitting the data graph into smaller but semantically similar and edge-disjoint sub-graphs. Given our observation that nodes with the same type often share similar type-neighborhoods, we induce a distinct set of partitions for G based on the types in G, using small sub-graphs surrounding vertices of the same type. The partitioning algorithm treats an input RDF dataset as a directed graph G concerning only the type information, i.e., we use the condensed view of an RDF graph. For any vertex that does not have a type specified by the underlying dataset, we assign an universal type NA to them.

D. **Query processing**

Query processing in the stored RDF files is done using SPAQL. Querying keyword is processed and values retrieved from RDF files. Search is first applied on the schema/summary of the data to identify promising relations which could have all the keywords being queried. Then, by translating these relations into search patterns in SPARQL queries and executing them against the RDF data, the actual sub graphs are retrieved. Efficiently values cab be retrieved from every partition from the data by collaboratively using SPARQL query and any RDF store.

E. **PRIVACY COMPATIBILITY ALGORITHM**

The privacy compatibility algorithm is used for checking whether the data services are compatible or not. To access the resources from the web in the fast manner and providing the concealed information to users and a third party service without revealing of privacy sensitive information of user and providing the compatibility services to the user and other services. Some personal information may be gathered when you register. During registration, this model asks for certain personal information In Daas composition to check the privacy congeniality of privacy policy and privacy requirements the PCM algorithm checks the statements in PRs with the statements in PPs. To check the congeniality between the statements of two services S and S' we developed the PCM algorithm. The result of composition is a set of component Daas services which must be composed in a particular order depending on their access patterns.

INPUT: Statement of privacy policy
INPUT: Statement of privacy requirement
OUTPUT: If there is an in congeniality

for each rule set rs=rs' to be compatible
For i=1, if i<RS do
For j=1, j<PR do
For j=1, j'<PP do
If Aj' subset of Aj then
Aj is congeniality to Aj' and posses good level of trust else Inc (Aj , Aj')
Goto step 4
End.

5. EXPERIMENTAL RESULTS

i. Start the apache tomcat server and the internet explorer.
ii. Open the browser and give localhost: 8090

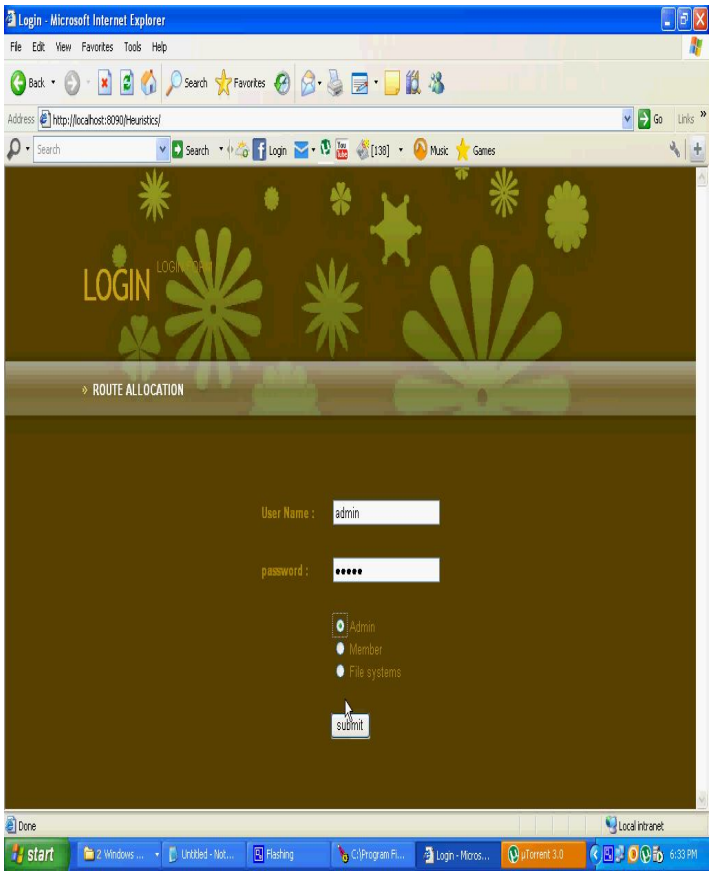


FIG 5.1: LOGIN PAGE

The above screen shows the login page where the admin can enter into the application by giving the name and password

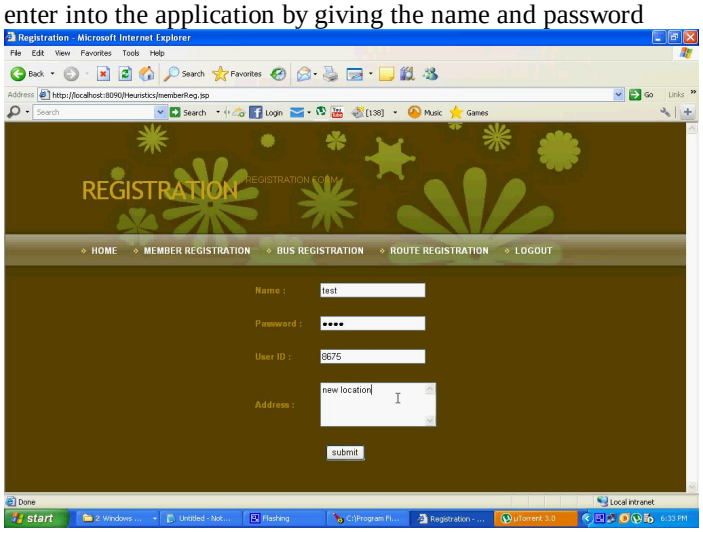


FIG 5.2: REGISTRATION PAGE

The above screen shows the registration page where the member enters the details by giving a user name and password. They can login into the application by using the username and password.

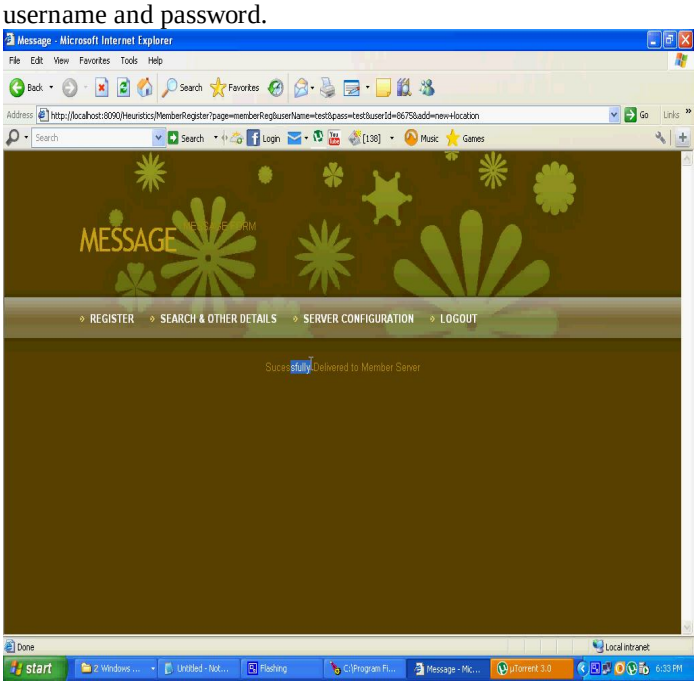


FIG 5.3 MESSAGE DISPLAYING PAGE

After admin enters the details of a member server into the distributed file system it displays a message as successfully delivered to the member server if not it displays the message failed to connect to the member server.

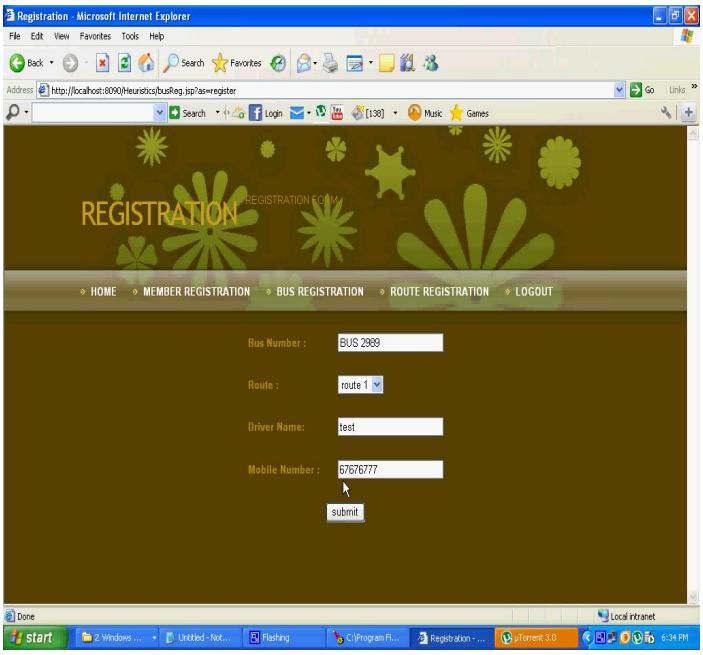


FIG 5.4: BUS REGISTRATION PAGE

The admin enters the details of a bus and submits to the distributed file system.

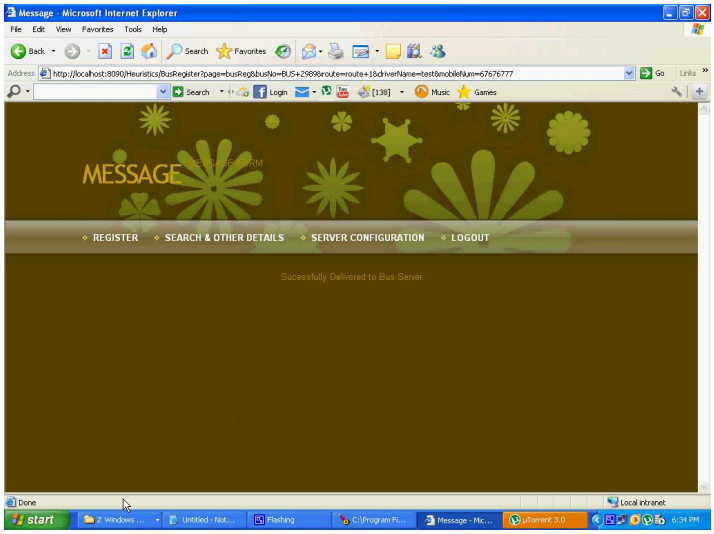


FIG 5.5: MESSAGE DISPLAYING PAGE

After the admin enter the details of a bus server into the distributed database it displays the message as successfully delivered to the bus server if not it displays failed to connect to the bus server.

6. CONCLUSION AND FUTURE WORK

The dynamic approach for enhancing privacy in web service composition goes beyond the previous privacy approaches and it ensures privacy compatibility of involved services in the composition without any additional overload. The dynamic approach for enhancing privacy in web service composition overcomes the two major short comings such as i.e., a service can only accept or refuse the other services, and the next one is once the producer designs a privacy policy it is given to all the interested services. This dynamic privacy model goes beyond the traditional data-oriented privacy approaches it does not reveal the privacy sensitive information.

Even though, privacy cannot be agreed as typical data, it can be agreed as a part of a privacy policy for specific purposes. They aim at designing techniques for protecting the composition results from privacy attacks before the final result is obtained. A standard frame work for performing queries on authenticated dictionary over the internet is provided by the web service interfaces. It also allows clients to spend less code which deals with serialization and communication of data by giving those tasks to already implemented standards. By conducting an extensive evaluation on Java based prototype, the performance of number of web services is evaluated. The suggestion is to enable the composition of DaaS services with privacy aware mechanisms that allow imposing individual privacy policies. The privacy of data can be protected by improving the attack methods and query conversion from stronger attacks

7. REFERENCES.

[1] Lalitha Devi katikala, Veera Swamy Anaparthy Dynamic Privacy model for protecting web service composition "International journal of Merging Technology and Advanced Reasearch In Computing .

[2] L. Zeng, B. Benatallah, A. H. H. Ngu, M. Dumas, J. Kalagnanam, and H. Chang. Qos-aware middleware for web services composition. *IEEE Trans. Software Eng.*, 30(5):311–327, 2004.

[3] M. Barhamgi, D. Benslimane, and B. Medjahed. Composing Data-Providing Web Services. *IEEE Transactions onServices Computing (TSC)*, 3(3):206–222, 2010.

[4]S.-E. Tbahriti, M. Mrissa, B. Medjahed, C. Ghedira, M. Barhamgi,and J. Fayn. Privacy-aware daas services composition. InA. Hameurlain, S. W. Liddle, K.-D. Schewe, and X. Zhou, editors, *DEXA (1)*, volume 6860 of *Lecture Notes in Computer Science*, pages 202–216. Springer, 2011.

[5] S. Ran. A model for Web services discovery with QoS. *SIGecom Exchanges*, 4(1):1–10, 2003.

[6] R. Vacul´ın, H. Chen, R. Neruda, and K. Sycara. Modelingand discovery of data providing services. In Proceedings of the2008 IEEE International Conference on Web Services, pages 54–61,Washington, DC, USA, 2008. IEEE Computer Society.

[7] M. Alrifai, D. Skoutas, and T. Risse. Selecting skyline services for qos-based web service composition. In *Proceedings of the 19th international conference on World wide web*, WWW '10, pages 11–20, New York, NY, USA, 2010. ACM.

[8] S.-E. Tbahriti, B. Medjahed, Z. Malik, C. Ghedira, and M. Mrissa. How to preserve privacy in services interaction. In L. Barolli, T. Enokido, F. Xhafa, and M. Takizawa, editors, *AINA Workshops*, pages 66–71. IEEE, 2012.

[9] M. Mrissa, S.-E. Tbahriti, and H.-L. Truong. Privacy model and annotation for DaaS . In G. A. P. Antonio Brogi, Cesare Pautasso, editor, *European Conference on Web Services (ECOWS)*, pages 3–10, Dec. 2010.

[10] B. C. M. Fung, T. Trojer, P. C. K. Hung, L. Xiong, K. Al-Hussaeni, and R. Dssouli. Service-oriented architecture for high-dimensional private data mashup. *IEEE Transactions on Services Computing*, 99(PrePrints), 2011.

[11] M. Barhamgi, D. Benslimane, and B. Medjahed. A Query Rewriting Approach for Web Service Composition. *IEEE Transactions onServices Computing (TSC)*, 3(3):206–222, 2010.

[12] Y. Gil, W. Cheung, V. Ratnakar, and K. kin Chan. Privacy enforcement in data analysis workflows. In T. Finin, L. Kagal, and D. Olmedilla, editors, *Proceedings of the Workshop onPrivacy Enforcement and Accountability with Semantics (PEAS2007)*
at ISWC/ASWC2007, Busan, South Korea, volume 320 of *CEUR Workshop Proceedings*. CEUR-WS.org, November 2007.