ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Protecting Web Service Composition From Privacy Attacks Using Dynamic Privacy Model

Ms.M.Sabrabeebe[1], Ms.C.Nancy Nightingale[2]

M.E., Department of Computer Science and Engineering, IFET College of Engineering, Villupuram[1]

Assistant Professor, Department of Information Technology, IFET College of Engineering, Villupuram[2]

ABSTRACT: Web service composition is a web technology that combines information from more than one source into a single web application. This technique provides a special type of composition application that aims at integrating data from multiple data providers depending on the user's request. In addition, DaaS (Data as a Service) composition may reveal privacy sensitive information. When enforcing a traditional privacy preserving model, such as privacy model and negotiation, the composed data would suffer from the problem known as the curse of privacy attacks. In this paper is used to propose a new dynamic privacy model in order to extend DaaS composition with privacy capabilities and to enable fast access to data resources on the Web. This dynamic privacy model makes it possible to dynamically reconcile the privacy capabilities of services when incompatibilities arise in DaaS composition. To validate the applicability of proposal through an implementation and a set of experiments.

KEYWORDS: Service Composition, DaaS Services, Privacy, Negotiation

I. INTRODUCTION

Web services have recently emerged as a popular medium for data publishing and sharing on the Web. A web service is a software function provided at a network address over the web or the cloud, it is a service that is "always on" as in the concept of utility computing .Thereby providing a well-documented, platform independent and interoperable method of interacting with their data. DaaS (Data-as-a-Service) Services where services correspond to calls over the data sources. DaaS eliminates redundancy and reduces associated expenditures by accommodating vital data in a single location, allowing data use and/or modification by multiple users via a single update point. Initially used in Web mashups, the DaaS strategy is often used by commercial organizations.

Data as a Service or DaaS is a cousin of software as a service. The emergence of service-oriented architecture (SOA) has rendered the actual platform on which the data resides also irrelevant. This development has enabled the recent emergence of the relatively new concept of DaaS. A service provider that enables data access on demand to users regardless of their geographic location. Also called Data as a Service (DaaS), data services are similar to Software as a Service in that the information is stored in the cloud and is accessible by a wide range of systems and devices. Data services can enable the data to be accessed and/or updated by multiple users while ensuring a single point for updates. Potential drawbacks to data services include server downtime from the data service provider, data loss in the event of a disaster, and the security of the data, both in its stored location and in the transmission of the data among users.

The DaaS approach delivers the following benefits:
Agility: Because data is easily accessible, customers can take immediate action and do not require in-depth understanding of actual data.
Affordability: Providers can construct a outsource in the presentation layer, which helps build highly affordable user interfaces and allows more feasible presentation layer change requests.
Data quality: Data accessibility is controlled through data services, which improves data quality, as there is a single update point.

1.1 Web Service composition

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Web service composition is a web technology that combines information from more than one source into a single web application. This technique provides a special type of composition application that aims at integrating data from multiple data providers depending on the user's request. The automatic selection, composition, and interoperation of Web services to perform some task, given a high-level description of an objective. A web service is any piece of software that makes itself available over the internet and uses a standardized XML messaging system. XML is used to encode all communications to a web service.

For example, a client invokes a web service by sending an XML message, then waits for a corresponding XML response. Because all communication is in XML, web services are not tied to any one operating system or programming language Java can talk with Perl; Windows applications can talk with Unix applications. Web Services are self-contained, modular, distributed, dynamic applications that can be described, published, located, or invoked over the network to create products, processes, and supply chains. These applications can be local, distributed, or Web-based. Web services are built on top of open standards such as TCP/IP, HTTP, Java, HTML, and XML. Web services are XML-based information exchange systems that use the Internet for direct application-to-application interaction.

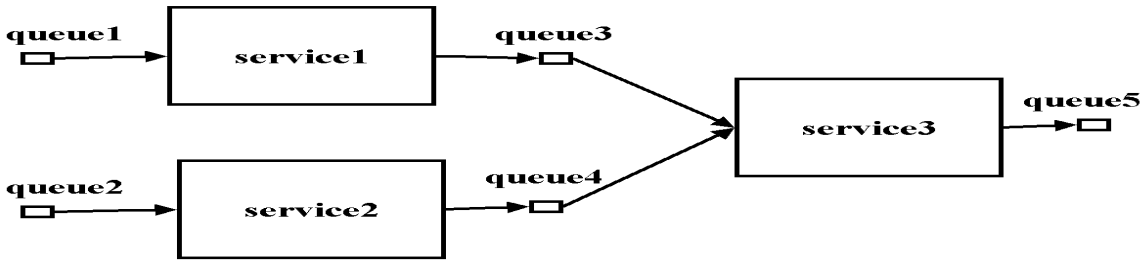

Fig.1. Service Composition

1.2 Challenges

Two factors exacerbate the problem of privacy in DaaS. First, DaaS services collect and store a large amount of private information about users. Second, DaaS services are able to share this information with other entities. Besides, the emergence of analysis tools makes it easier to analyze and synthesize huge volumes of information, hence increasing the risk of privacy violation. In the following, we use our epidemiological scenario to illustrate the privacy challenges during service composition.

Challenge 1: Privacy Specification. Let us consider services S4.1 and S5.1 in. The scientist considers both input and output parameters of S4.1 (i.e., SSN and DNA) as sensitive data. Let us now assume that this scientist states the following hypothesis: "weather conditions" has an impact on H1N1 infection." For that purpose, he/she invokes S5.1. The scientist may want to keep S5.1 invocation as private since this may disclose sensitive information to competitors. The aforementioned first challenge puts in evidence the need for a formal model to specify private data is and how it will be defined.

Challenge2: Privacy within compositions. Component services (that participate in a composition) may require input data that cannot be disclosed by other services because of privacy concerns. They may also have conflicting privacy concerns regarding their ex- changed data. For instance, let us assume that S1.1 states to disclose its data (SSN) to a third-party service for use in limited time. S3.1 meanwhile attests that it uses collected data (SSN) for an unlimited time use. Then, S1.1 and S3.1 have different privacy constraints regarding the SSN. This will invalidate the composition in terms of privacy concerns.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Challenge 3: Dealing with incompatible privacy policies in compositions. The role of the mediator is to return composite services with compatible component services with respect to privacy.

1.3 Contributions

Dynamic Privacy Model: This model deals with privacy in the web service composition. To protecting the composition results from the privacy attacks before the final result is returned to the user.

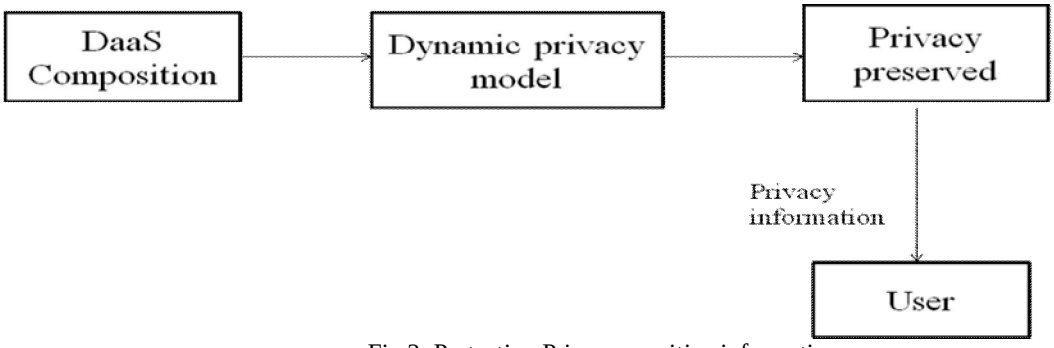

Fig.2. Protecting Privacy-sensitive information

DaaS Composition: Data as a Service (DaaS) is an information provision and distribution model in which data files (including text, images, sounds, and videos) are made available to customers over a network, typically the Internet. DaaS offers convenient and cost-effective solutions for customer- and client-oriented enterprises. DaaS eliminates redundancy and reduces associated expenditures by accommodating vital data in a single location, allowing data use and/or modification by multiple users via a single update point. Initially used in Web mashups, the DaaS strategy is often used by commercial organizations. Data as a Service or DaaS is a cousin of software as a service (SaaS). The emergence of service-oriented architecture (SOA) has rendered the actual platform on which the data resides also irrelevant.

This development has enabled the recent emergence of the relatively new concept of DaaS. The service provider that enables data access on demand to users regardless of their geographic location. Also called Data as a Service (DaaS), data services are similar to Software as a Service in that the information is stored in the cloud and is accessible by a wide range of systems and devices. Data services can enable the data to be accessed and/or updated by multiple users while ensuring a single point for updates. Potential drawbacks to data services include server downtime from the data service provider, data loss in the event of a disaster, and the security of the data, both in its stored location and in the transmission of the data among users.

Privacy Compatibility Checking: Capable of both assessing the compatibility and identifying incompatibility of service. Some personal information may be gathered when you register. During registration, this model asks for your email address and certain other personal information.

Privacy Compatibility Matching: To check the privacy compatibility of privacy policy and privacy requirement.PCM check the in assertions in Privacy Requirements with assertion in Privacy Policy for example assertion is service feature, preference, capability and requirements.

Negotiation to Reach Compatibility: The mediator basically discards any composition plan which is subject to privacy incompatibility from the set response. The main idea behind avoiding empty responses is to reach a compatible through a privacy-aware negotiation mechanism. Dynamically reconcile the privacy capabilities of services when incompatibilities arise in a composition.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

II. FORMAL MODEL FOR PRIVACY SPECIFICATION

A. Privacy Specification Model

In order to define an expressive model of privacy for web services, it is necessary first to examine the nature of data and to formally describe what we mean by privacy so that can argue that we protect such private data. In this case, the term privacy relates to the right of an entity to determine why, for whom, and for how long some information should be released. Due to the privacy subjectivity, each service has to identify which data are considered as *private* (noted as *rs*). If *S* provides some private data *rs*, then a set of privacy requirements applies to *rs*, and if *S* collects some private data *rs*, then a set of privacy policies also applies to *rs*.

1) *Privacy Rule:* A privacy rule *Ri* is defined by a tuple (*Ti*, *Di*, *Gi*) where *Ti* is the topic of *Ri* giving the privacy facet. For instance, the topic can describe: 3 *purpose*, *recipient*, or *retention*. *Purpose* topic states the intent for which a given private data *rs* (collected or provided by *S*) will be used; the *recipient topic* mentions if and to whom *rs* can be revealed the *retention* topic specifies until when *rs* is stored by a third-party service. Then, for each topic *Ti*, a set *Di* defines the value domain of the topic. The definition of *Di* is based on an ontology domain. For example, we consider the privacy rule*R*1 that corresponds to the topic *T*1 = *recipient* and the domain*D*1 = *{public*, *government*, *private-lab*, *research-lab*, *hospital*, *university}*. To define *Gi ={total*, *partial}* as a granularity indicator, which states whether or not the data in *rs*, to which *Ri* applies, represent the totality of the service input or output. In this paper, for the sake of simplicity, we only consider the case where *Gi=total*.4 The definition of privacy rules, called *Rule Set* (*RS*), is described independently of any private data.

2) *Privacy Assertion:* The application of a rule *Ri* = (*Ti*, *Di*, *Gi*) to private data *rs* is a privacy assertion noted as *A*(*Ri*, *rs*) = *pf*. *S* specifies its privacy concerns for *rs* through *A*(*Ri*, *rs*). For example, let consider *rs=DoB* and *R*1 which corresponds to the topic *T*1 =*recipient* and the domain *D*1. A privacy assertion applied to *rs* = *DoB* through *R*1, which states that *rs* will be shared with *government* agencies and *research-lab*.

3) *Privacy Requirements PRS:* A service *S* providing some private data *rs* as its output specifies a set of privacy requirements, denoted as *PRS*, in terms of usage expectations.

4) *Privacy Policy PPS:* A service *S* requesting some private data *rs'* (where *rs'* = *rs* referring output data of *S*)as input specifies its privacy policy, noted *PPS*, stating how *S* is going to use *rs'*.

B. Privacy Annotation for DaaS

The web service description language (WSDL) standard gains considerable momentum as the language for web service description. However, WSDL provides no support for privacy description of services. Existing standards such as WS-security focus on "on an access control-oriented of privacy and do not offer the possibility for describing requirements and policies as with our model. Moreover, policy adaptation is not supported. In order to describe the privacy concerns of web services [8]. To exploit its extensibility elements to associate service operations, inputs, and outputs with their corresponding *PRS* and *PPS*. More precisely, we extend the *operation*, *input* and *output* elements with a *privacy-reference* attribute that contains a link to a privacy file, thus keeping a clear separation between the functional description of the service and its privacy concerns.

III. SYSTEM ARCHITECTURE

The approach presented in this paper is implemented as a project which deals with the privacy preservation issue in P2P data sharing environments. This research where the need of data sharing is apparent for making better a health environment of people. To support the decision process multiple data sources such as the patient data, his social conditions, the geographical factors, etc. The data sources are provided by DaaS services and are organized with peers. DaaS services differ from traditional Web services, in that they are stateless i.e. they only provide information about the current state of the world but do not change that state.

When such a service is executed, it accepts from a user an input data of a specified format ("typed data") and returns back to the user some information as an output. DaaS services are modeled by RDF views. Figure 3 summarizes the architecture of this project. The Multi-Peer Query Processing component is in charge of answering the global user

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

query. The latter has to be split local queries (i.e., sub-queries) and has to determine which peer is able to solve a local query. Each sub-query is expressed in SPARQL. Each peer handles a Mediator equipped with a Local Query Processing Engine component. The mediator exploits the defined RDF views within WSDL files to select the services that can be combined to answer the local query using an RDF a query rewriting algorithm [2]. Then, it carries out all the interactions between the composed services and generates a set of composition plans to provide the requested data.

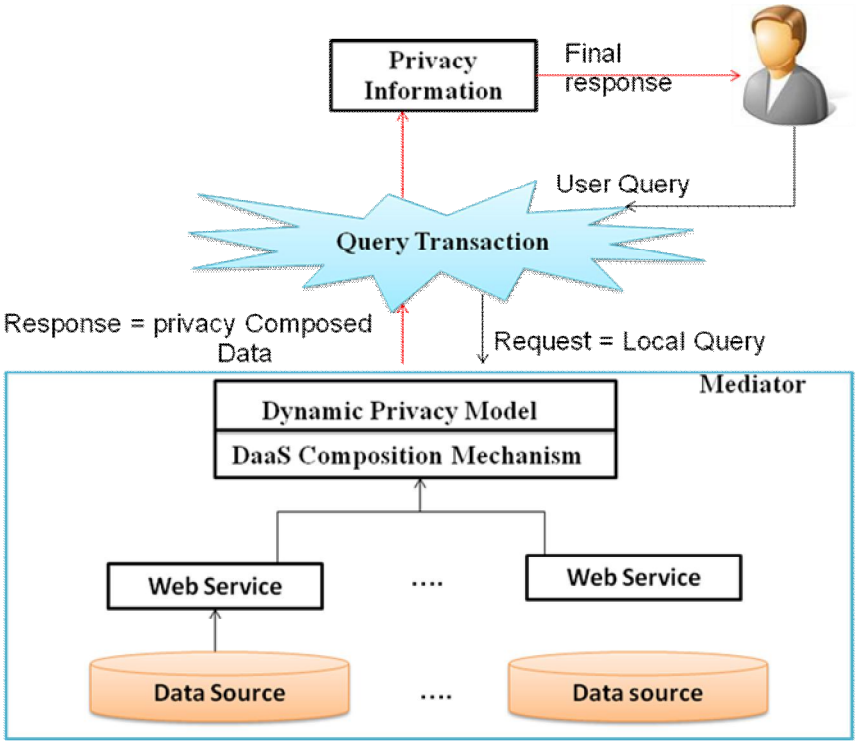

Fig .3. System Architecture

Then, it carries out all the interactions between the composed services and generates a set of composition plans to provide the requested data. It deals with privacy not only at the data level (i.e., inputs and outputs) but also service level. In this paper to build upon this model two other extensions to address privacy issues during DaaS composition. The privacy model described in this paper is based on the model.

IV. DAAS COMPOSITION

To Combines information from more than one service into a single web application. Combining data from different sources could potentially reveal privacy-sensitive information. To securely integrate data from different sources could potentially reveal privacy-sensitive information. To securely integrate private data from different data providers, whereas the integrated data still retains the essential information

A web service is any piece of software that makes itself available over the internet and uses a standardized XML messaging system. XML is used to encode all communications to a web service. For example, a client invokes a web service by sending an XML message, and then waits for a corresponding XML response. Because all communication is in XML, web services are not tied to any one operating system or programming language--Java can talk with Perl; Windows applications can talk with Unix applications. Web Services are self-contained, modular,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

distributed, dynamic applications that can be described, published, located, or invoked over the network to create products, processes, and supply chains.

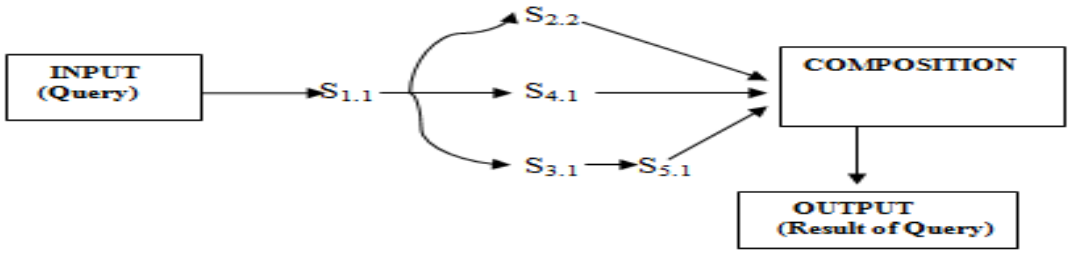

Fig.4. Composition Plan

V. THE PRIVACY COMPATIBILITY CHECKING

This method is Capable of both assessing the compatibility and identifying incompatibility of service. Some personal information may be gathered when you register. During registration, this model asks for your email address and certain other personal information. To introduce the notion of compatibility between privacy policies and requirements. Then define the notion of privacy subsumption and present our cost model based privacy matching mechanism.

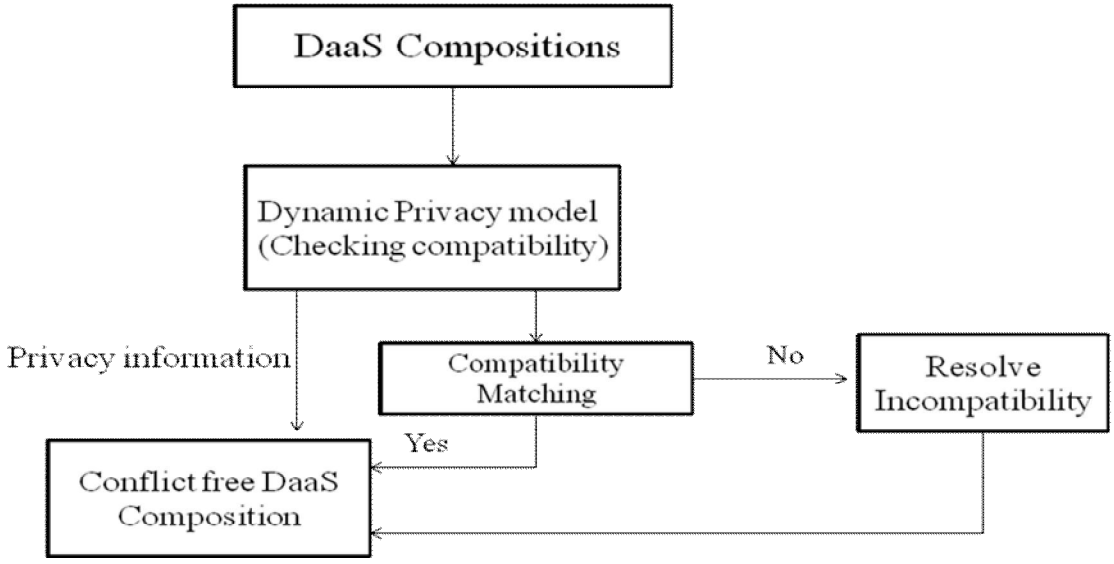

Fig .5.Compatability Checking

VI. PRIVACY COMPATIBILITY MATCHING

To check the privacy compatibility of privacy policy and privacy requirement in DaaS Composition Privacy Compatibility Matching (PCM) check the in assertions in Privacy Requirements(PR) with assertion in Privacy Policy (PP) The example of assertion are service feature, preference, capability and requirements.

6.1PrivacySubsumption: Let us consider a rule Ri = (Ti,Li,Di,Si). Defining an assertion A(Ri, rs) =(pf, g) for involving assigning value(s) from Di to the propositional formula pf of A. The value in Di. are related to each other.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Algorithm1: *PCM*
Input: PRS = {(Aj(Ri,rsk)),j<=|PRS|, i<=|RS|, k<=|Pc|, rsk∈PRi∈RS}(assertion of privacy requirements)
input: PPS'={(Aj(Ri,rsk)), j<=|PPS'|, i<=|RS|, k<=|Pp|,rsk∈Pp,Ri∈RS}(assertion of privacy policy)
output: InC (These to find compatible assertion Couple)
Step 1: for i=1,i<=|RS|do
Step 2: for j=1,j<=|PRS|do
Step 3: for j=1,j<=|PPS'|do
Step 4: if(Aj(Ri,rsk)∈(Aj(Ri,rsk)then
Aj(Ri,rsk)is compatible with
Aj(Ri,rsk)
elseInC←(Aj(Ri,rsk)
Then goto step1
Step5: End.

VII.NEGOTIATION TO REACH COMPATIBILITY

The mediator basically discards any composition plan which is subject to privacy incompatibility from the set response. The main idea behind avoiding empty responses is to reach a compatible through a privacy-aware negotiation mechanism. Dynamically reconcile the privacy capabilities of services when incompatibilities arise in a composition. Compared to, in this paper, we revise the previous idea of negotiation and provide many improvements. The negotiation decision is cautiously taken according to a utility-based cost function defined by a service provider.

VIII. CONCLUSION AND FUTURE WORK

In this paper, the proposed a dynamic privacy model for web services. This model deals with privacy at the DaaS. Composition to tackle the incompatibilities between privacy policies and requirements. Further, dynamic privacy must reveal with privacy sensitivity information whenever the privacy attack occur. Although privacy cannot be carelessly negotiated, it is still possible to negotiate apart of privacy policy for specific purposes. In any case, privacy policies always reflect the usage of private data as specified or agreed upon by service providers. As a future work, the aim at designing technique for protecting the composition results from privacy attacks in cloud computing.

REFERENCES

[1] Salah-Eddine Tbahriti, Chirine Ghedira, Brahim Medjahed and Michael Mrissa.Privacy-Enhanced Web Service Composition. IEEE Transactions on Services Computing , March 2013 .
[2] M. Barhamgi, D. Benslimane, and B. Medjahed. A Query Rewriting Approach for Web Service Composition. IEEE Transactions on Services Computing (TSC), 3(3):206–222, 2010.
[3] G. T. Duncan, T. B. Jabine, and V. A. de Wolf, editors. Private lives and public policies: confidentiality and accessibility of government statistics. National Academy Press, Washington, DC, USA, 1993.
[4] B. C. M. Fung, T. Trojer, P. C. K. Hung, L. Xiong, K. Al-Hussaen, and R. Dssouli. Service-oriented architecture for high-dimensional private data mashup. IEEE Transactions on Services Computing, 99 (PrePrints), 2011.
[5] 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 on Privacy Enforcement and Accountability with Semantics (PEAS2007)at ISWC/ASWC2007, Busan, South Korea, volume 320 of CEUR Workshop Proceedings. CEUR-WS.org, November 2007.
[6] Y. Gil and C. Fritz. Reasoning about the appropriate use of private data through computational workflows. In Intelligent Information Privacy Management, Papers from the AAAI Spring Symposium, pages 69–74, March 2010.
[7] B. Hore, S. Mehrotra, and G. Tsudik. A privacy-preserving index for range queries. In Proceedings of the Thirtieth international conference on Very large data bases - Volume 30, VLDB '04, pages720–731. VLDB Endowment, 2004.
[8] M. K¨ahmer, M. Gilliot, and G. M¨ uller. Automating privacy compliance with expdt. In Proceedings of the 2008 10th IEEE Conference on E-Commerce Technology and the Fifth IEEE Conference on Enterprise Computing, E-Commerce and E-Services, pages 87–94,Washington, DC, USA, 2008. IEEE Computer Society.
[9] H. Kargupta, K. Das, and K. Liu. Multi-party, privacy-preserving distributed data mining using a game theoretic framework. In Proceedings of the 11th European conference on Principles and Practice of Knowledge Discovery in Databases, PKDD 2007, pages 523–531, Berlin, Heidelberg, 2007. Springer-Verlag.