International Journal of Hybrid Information Technology
Vol.8, No.8 (2015), pp.385-392
http://dx.doi.org/10.14257/ijhit.2015.8.8.38

# Analysis of Privacy Protection Model under Web Service Composition Framework

Wang Wang[1], Huang Zhiqiu[2] and Peng Huanfeng[3]

*[1,2,3]College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, 210016, China*
*[3]School of Computer Engineering, Nanjing Institute of Technology, Nanjing, 211167, China*
*njwangwang1988@163.com*

***Abstract***

*The privacy protection model under Web service composition framework is studied in depth, then the privacy of customers can be protected effectively. Firstly, the basic framework of Web service composition is studied; Secondly, the managing method of service publication is analyzed; Thirdly, the privacy protection model under Web service composition framework is discussed; finally the evaluation method of algorithm for privacy protection is summarized.*

***Keywords:*** *privacy protection model; Web Service Composition Framework; algorithm; evaluation*

## 1. Introduction

Service oriented computing can make enterprise application change with requirement, the core idea is that quickly construct the loose coupling distributed application system based on service composition using service as basic unit. With constant mature and development of Web service, the service oriented computing has obtained good technical support. Web service composition framework has been concerned by many scientists at abroad and home. The Web service standard improved continuously and the enterprise software platform supporting the Web service matures also, more and more enterprises and business organizations participate in Software as a Service, and issues the standard Web service making up of business function and components, then they can find out partners quickly, and searches potential customers, and improve the value of business. However the services online have some disadvantages, such as simple structure, and single function, which can not satisfy the complex requirement of enterprise [1].

Collaboration system based on Web service usually relates to a group of different organization that participates in the service, they want to achieve the common goal, and then they carry out information sharing and mutual cooperation. But the open service environment has the characteristics of self-rule dynamic state and isomerism, then the activity credibility of interacting two sides has difficulty in ensured, the personnel and sensitive data of Web service customer exists the risk of illegal collection and disclosure. For example, if the enterprise does not carefully screen issued data, the business competitor can get an opportunity, therefore the Privacy protection has been studied by some scientists in recent years. The privacy protection technology can deal with the disadvantages of Web service composition framework mentioned above, there are two aspects should be considered during the procession of executing privacy protection, firstly, how to avoid the leakage of privacy during the procession of data application, secondly, how to benefit the application of data, the current researching hotspot focuses on the design of privacy protection principle and algorithm.

ISSN: 1738-9968 IJHIT

## 2. Basic Framework of Web Service Composition

There are many achieving technologies of Web service composition, and it is difficult to establish the united framework of Web service. An achieving framework of classic Web service composition framework based on Web service composition theory was put forward, which can summarize the Web service composition technology [2]. This kind of framework is made up of two parts (service requester and service provider) and five parts (translator, composition manager, execution engine, service matching device, service library), these parts can complete coordinately composition task of Web service, and the Web service composition framework diagram is shown in Figure 1.

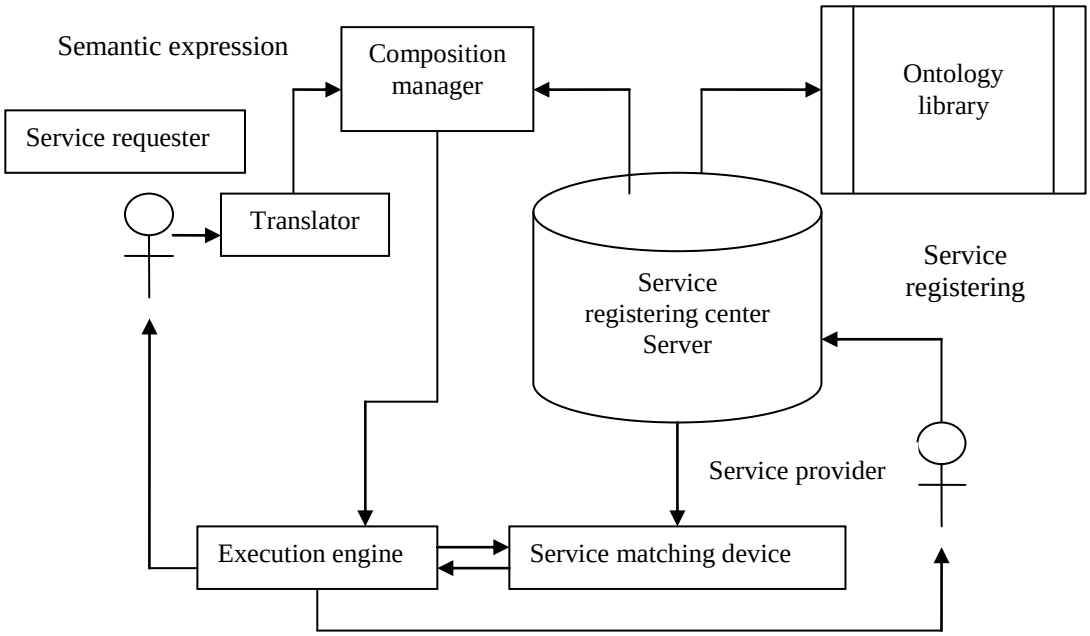


**Figure 1. Classic Web Service Composition Framework Diagram**

The executing procedures of Web composition is listed as follows:

Step 1: the service provides the service firstly, and carries out service registering based on service registering center server, this is the prerequisite of carrying out Web service composition;

Step 2: Service requester use the service, which should submit the requirement description of the natural language. The description can be translated based on translator, the natural language can be transferred to semantic information that can be identified by the computer the semantic information can be transmitted to the composition service manger.

Step 3: the composition service manger can carry out composition of service according to the description submitted by service requester, and then final generating composition plan can be transmitted to the execution engine.

Step 4: the execution engine transfers the composition plan to service matching device, the service matching device search the current Web service information description, such as Qos describing information, and carries out the matching with requested information,

 

then the proper Web service can be confirmed, the final results can be fed back to the execution engine.

Step 5: the execution engine confirms the service series according to the service match device, and calls corresponding Web service, the final execution results can be transferred to service requester.

## 3. Managing Method of Service Publication

Traditional service composition platform and its service publication means have two main types, one is distributed function, every device should find out the business satisfies the request of enterprise, the other is function centralization, a controlling center manages all resources of system, and response to the request of customer [3]. However, under Web service environment a lot of computing device is made up of different computing resources, and there are big differences among them, and these computing devices has the characteristics of mobility and service dynamics, therefore the traditional Web composition means do not satisfy the requirement. In recent years, an advanced service composition method is put forward based on hierarchical structure.

(1) Performance difference classification

According to the performance difference of device online, the devices can be divided into four levels: low level (L1), original level (L2), middle level (L3), and high level (L4).

The service of low level device has not the ability of issuing service, which can complete business with help of high level device, such as simple sensor, printer. The original level device has host computing of software module, which can offer outward service, such as intelligent sensor. The middle level device has the mobility, which not only offers outward service, but also issues service, such as computer, and intelligent cell phone. The high level devices has same function with middle level devices, which has more strong computing ability, it is fixed device, such as server.

(2) Generation protocol of Web composition framework

A service organization method with hierarchical structure is constructed based on the dividing standards of devices mentioned above. When a device A enters into the service system, it issues broadcast message (concludes classified level L(A) of device A), waits for response of service device in nearby system. The device B receives the broadcast massage, and carries out comparison according to its level L(B) [4].

If $L(A)<L(B)$, device B issues information, the device A is informed to set itself as father node.

If $L(A)>L(B)$, device B issues information, it agrees to be the sub node of device A;

If $L(A)=L(B)$, device B issues information, it agrees to be brother node of device A.

The basic generating principle of hierarchical structure is listed as follows: any device has one (and only one) father node. When a device has a node of father device, it should refuse the information of other upper level device node.

(3) Service search and composition

The service loading module is the software of middle and high level device, searching service region in service loading module of middle level device concludes the service management region of father node. The searching service region in service loading module of high level device is service management region of all nodes of high level device.

The service management region concludes devices and all services issued by sub node device. These services are stored in UDDI, every middle or high level device can manage the description information issued by service based on UDDI. When the node of device needs to add or delete service, the IN FO_ADD information and IN FO_REMOVE information can be published through the upper level device node. When service loading module issues request for UDDI, the range of searching results returned by UDDI belongs to service searching range. When service loading module carries out matching with service, firstly the comparing and matching among all services offered by system and customer requirement defined in document through procession are carried out, and then the possible searching results are returned to UDDI.

(4) Service changes and updates

Under Web service composition framework, it is important to reduce the effect of changes of service framework on the system. The device under Web service composition framework may stop to offer outward service because of mobility of device. For example, PDA or personnel computer of customers move from one place to another place, or the power of mobile device is insufficient.

Single Web service can only provide the limited function, in order to apply the sharing Web service effectively, it is necessary to put the sharing Web services together, then the service function can be improved. The business process execution language can describe the execution of business procession, is an effective tool of Web service composition. BPEL confirms a procedure structure, and calls a Web service, defines and transfers data in procedure. In actual application, BPEL can not solve all problems under Web open environment service composition. During the procession of designing stage of composition service, the proper member services can be found out through effective searching mechanism, however at present BPEL composition service keeps a static binding relationship, therefore the structure of it is difficult to be regulated dynamically, when the environment changes, composition relationship only be rebuilt and described. Some scientists established a dynamic Web service composition framework structure. This framework is constructed based on BPEL language and UDDI protocol, the extensive Qos components are used, the supporting business procedure binds with Web service dynamically during operating stage, under abnormal condition the system can be revised dynamically, then the execution efficiency of business procedure can be improved.

## 4. Privacy Protection Model under Web Service Composition Framework

The classic privacy protection model is established centered customer, which is made up of privacy setting module and privacy processing module. The corresponding diagram of privacy protection model is shown in Figure 2.

 

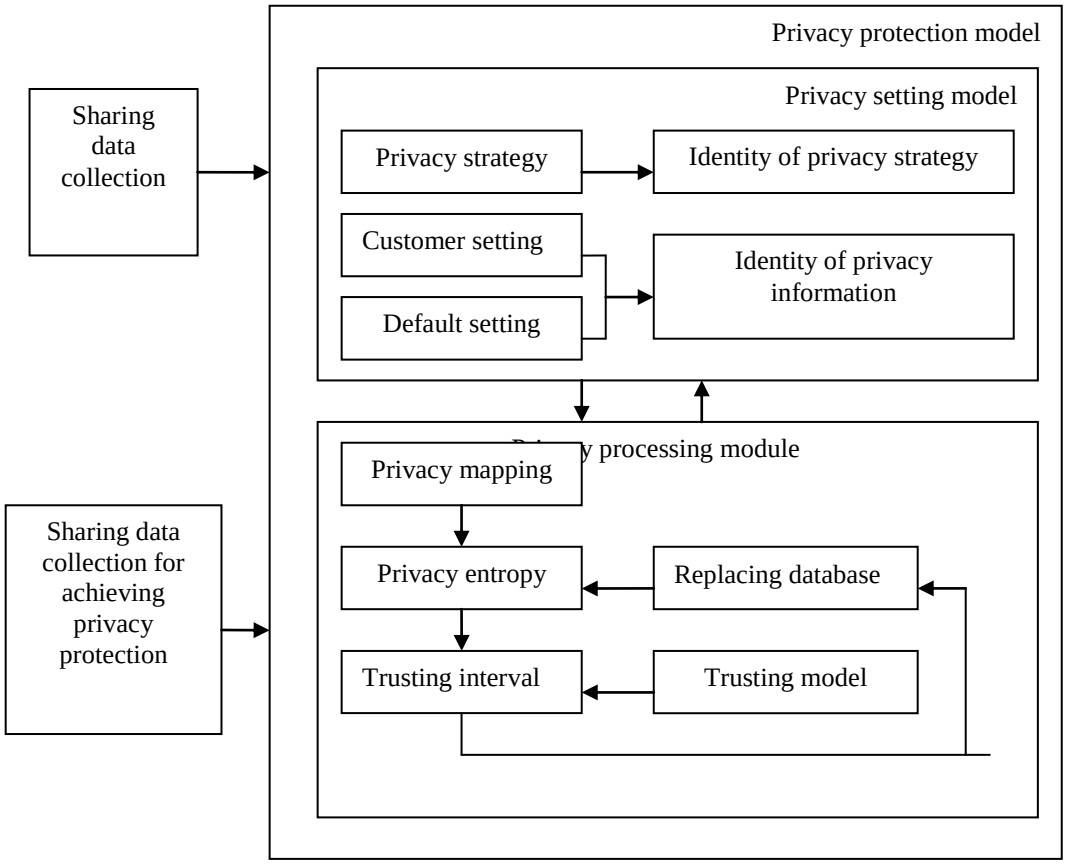


**Figure 2. Diagram of Privacy Protection Model**

(1) Privacy setting module

This module concludes customer setting and default setting, which can complete the function of setting privacy range, where default setting defines the public information needed to be protected under Web service composition framework as privacy information. In the part of customer setting, the customer can set the critical word and feature of privacy information. The privacy preference of customer concludes privacy information type, time boundary and space boundary, which can offer a application interface of user privacy preference and a setting interface. The customer can set the privacy according to the preference of himself. The critical word and feature collections in the semantic form can be obtained after the privacy settings [5].

(2) Privacy processing module

This module can process the sharing data of customers and protect the privacy, the corresponding procession is listed as follows [6]:

Step 1: find out information with privacy, the sharing data collections are scanned based on information processing method, which are defined as $D_s(D_1, D_2, \cdots, D_t)$ ( $t \le m$ ), a privacy mapping function $P$ is introduced, $P :\to \{0.1\}$ denotes a judgment that the sharing data of customer concludes the privacy, $d_1, d_2, \cdots, d_r \in \{0,1\}$ ( $d_j = P(D_j)(j = 1,2,\cdots,r)$ ) denotes the function value of $P$ , where $d_j = 1$ denotes that the data $D_j$ concludes privacy; $d_j = 0$ denotes that the data

$D_j$ does not conclude privacy. If $d_l = P(D_l) = 1(l = 1, 2, \cdots, m)$, $d_l$ is introduced into collection $d'$.

Step 2: calculate the privacy information entropy

The privacy information entropy $h(D_j)$ is calculated for every data in collection $d'$, then the information entropy concluding privacy information in data sharing collection is calculated by the following expression:

$$H' = \sum_{j=1}^{\omega} H(D_j) H(D_j) = -k(\sum_{j=1}^{n} P_i \log P_i) \tag{1}$$

Step 3 divide the interval, a trust-privacy mapping function $T$ is introduced, $T: D \to (a, b)$, denotes mapping of the identity trusting interval $T$ to available privacy information quantity. There are $u$ trusting intervals $T$, every trusting interval control $v$ privacy information $Q$, $t_i \in T$, $q_j \in Q$ denotes the trusting interval $t_i$ controls $q_j$ privacy information. The down and up limits can be calculated by the following expressions [7]:

$$a_i = \frac{1}{u}(l-1)\sum_{i=1}^{u}\sum_{j=1}^{v} H(q_j) \tag{2}$$

$$b_i = \frac{1}{u} l \sum_{i=1}^{u}\sum_{j=1}^{v} H(q_j) \tag{3}$$

where $l = 1, 2, \cdots, u$.

Step 4: replace and share, for sharing data of customers, if $H' \in (a_i, b_i)$, the privacy entropy of this sharing collection belongs to available privacy entropy interval of sharing objects, the data collection can be shared. If $H' \notin (a_i, b_i)$, the data in sharing data collection can replace data of database until the following condition $H' \in (a_i, b_i)$ is satisfied, then the new data collection is shared. The replacing times can be confirmed according to computing environment and application view.

## 5. Evaluation Method of Algorithm of Privacy Protection

The evaluation method of algorithm of privacy protection has the following four kinds [8]:

(a) Protection degree of privacy, the index can be calculated by the "disclosing risk", the less the disclosing risk is, the higher the privacy protection degree is.

(b) Utility of data, it can be used to measure the quality of privacy protection data distributed, the higher the missing data is, the more the missing information is, the lower the utility of data is.

(c) Algorithm performance, data computation overhead (time complexity) and data communication are important indexes of measuring the algorithm performance.

(d) Applicability of algorithm, it can be used as the important index that can describe applicability of different algorithm to the application environment.

Three kinds of data mining methods for privacy protection have different characteristics, under different application requirement the application range and performance of them are different, which can be shown in Table 1.

 

**Table 1. Performance Evaluation of Data Mining Method of Privacy Protection**

| Method | Protection degree of privacy | Data utility | Computing overhead | Communication overhead |
|---|---|---|---|---|
| encryption technology | High | High | High | High |
| data distortion | Medium | Low | High | Low |
| data anonymization | Low | Medium | Medium | Low |

## 6. Conclusions

The Web service composition framework that is applied in privacy protection has been studied by many scientists, the effective privacy protection strategy should be applied in system, and the data of customer needed by Web service is managed uniformity, the data of customer can avoid illegal disclosure, then the privacy of customer can be protected effectively. Under Web service composition environment, the privacy protection problems can be coped with better. The confidentiality, correctness, efficiency and extendibility of current privacy protection model have still disadvantages, and a united evaluation system and quantization standard should be found out.

## References

[1] D. Shui-Guang, H. Long-tao and Y. Jian-wei, "Technical framework for Web Services composition and its progress", Computer Intergrated Manufacturing Systems, vol. 17, no. 2, **(2011)**, pp. 404-412.
[2] Y. Qing-Tao and C. Yan-ping, "Survey on Web Services Composition Methods, Computer Knowledge and Technology", vol. 6, no. 7, **(2010)**, pp. 1585-587.
[3] G. Walid, B. Karim and G. Claude, "Log-based mining techniques applied to Web service composition reengineering", Service Oriented Computing and Applications, vol. 2, no. 2-3, **(2008)**, pp. 93-110.
[4] D.-J. Lee, J.-H. Ahn and Y. Bang, "Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection", MIS Quarterly, vol. 35, no. 2, **(2011)**, pp. 423-444.
[5] G. Jie, X. Jia-yun and B. Jia-li, "Region of Interest Based Selective Encryption Scheme for Privacy Protection in H.264 Video", Journal of Shanghai Jiaotong University(Science), vol. 19, no. 4, **(2014)**, pp. 385-391.
[6] K. G. Shin, X. Ju and Z. Chen, "Privacy protection for users of location-based services", IEEE Wireless Communications, vol. 19, no. 2, **(2012)**, pp. 30-39.
[7] O. Abul, F. Bonchi and M. Nanni, "Anonymization of moving objects databases by clustering and perturbation", Information systems, vol. 35, no. 8, **(2010)**, pp. 884-910.
[8] N. Wei-wei, Z. Jin-wang and C. Zhi-hong, "HilAnchor-Location privacy protection in the presence of users' preferences", Journal of Computer Science & Technology, vol. 27, no. 2, **(2012)**, pp. 413-427.

## Author

**Author's Name: Wang Wang**

Author Affiliation(s): College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics

Research direction: Web services privacy and information security.