Web Service Locating Unit in RFID-centric Anti-counterfeit System

Zhiyuan Tan, Xiangjian He and Priyadarsi Nanda
Centre for Innovation in IT Services and Applications (iNEXT)
University of Technology, Sydney
Sydney, Australia
{thomas, sean, pnanda}@it.uts.edu.au

Abstract—**The problem of piracy has disturbed people's daily life for hundreds of years and has not been relieved until now, though many existing anti-counterfeit solutions have been applied. However, due to the emergences of Radio Frequency IDentification (RFID) technologies, there is a more reliable alternative solution to construct authentication system. On the other hand, there arises another issue of how to simplify the deployment of RFID-centric anti-counterfeit system over the Internet. In this article, we propose an approach, Web Service Locating Unit (WSLU), to achieve this goal to manage numbers of RFID-centric authentication services (relied on web services).**

Keywords-Web Service; Radio Frequency Identification; authentication

I. INTRODUCTION

Radio Frequency IDentification (RFID) [13] is a powerful identification technology and has been widely adapted to various fields such as Anti-counterfeit, Logistic, Health Care and Electronic Ticket. The special features of RFID technology, such as tag authentication, stand fire, antimagnetic and waterproof, facilitate its implementation in anti-counterfeit applications. However, there are some issues that have been arisen when implementing and operating RFID-centric anti-counterfeit system. One of the topics receiving most concern is how to effectively integrate the RFID-based authentication units with authentication services which may run on different platforms and be developed using various programming languages. In this paper, Web Service Locating Unit (WSLU), a Web service technology is proposed to achieve an RFID-centric anti-counterfeit system which makes a seamless integration of RFID-based authentication units into diverse authentication services. WSLU provides automatic Web services locating and Web services subscribing. This article is organized as follows. Section Ⅱ discusses a related study in middleware technologies to dynamic Web services. The detailed description of WSLU is presented in Section Ⅲ. Section Ⅳ is devoted to the concepts and the architecture of RFID-centric anti-counterfeit system. In Section Ⅴ, we show the architecture outcome followed by the experimental results of RFID-centric anti-counterfeit system in Section Ⅵ. We present the summary of our work and conclude our achievements in Section Ⅶ.

II. RELATED WORK

The emergence of Web service technology simplifies the interaction of applications in web environment. Increasing number of enterprise systems leads to public system functionalities or integration of external services via Web services. Therefore, intelligent Web services have become highly demanded. Noh-sam and Gil-haeng [17] introduced an Agent-based Web Services Middleware (AWEM) to facilitate service consumers to acquire "dynamic and effective result from Web services" according to their preference. AWEM assigns an appropriate Web service to a consumer based on the specified keywords and consumer's preferences. According to the authors of [17], AWEM is made up of five components, namely controller, Web services agent server, template generator, Web services agent and Web services cache. This approach does not address some issues such as access control, load balance and challenge of Web services change.

III. WEB SERVICE LOCATING UNIT

In order to provide powerful authentication functionality, large amount of potential authentication services coming from diverse service providers will be integrated into a RFID-centric anti-counterfeit system. Therefore, there is enormous service information to be managed. For a low performance RFID-based authentication unit, it is a big challenge to maintain this service information. Moreover, every single change of a service will lead to a high cost for maintaining the consistency of the whole RFID-centric anti-counterfeit system.

As for authentication service provider, it will create a lot of redundant data in the provider's servers because the servers need to maintain the information of every authorized RFID-based authentication unit to prevent illegal access. Therefore, Web Service Locating Unit (WSLU) is an indispensable component to the RFID-centric anti-counterfeit system. Nevertheless, the WSLU can achieve effective system load balance.

A. Two-way Web service

Web service technology is a solution for achieving loose corporation between various platforms and systems. It employs the idea of Service-Oriented Architecture (SOA) to the interaction of existing disparate enterprise applications [11]. Web service follows several industry standards which

are **UDDI** (Universal Description, Discovery and Integration) [9], **WSDL** (Web Services Description Language) [4] and **SOAP** (Simple Object Access Protocol) [2].

Different from the conventional one-way Web service, whose request is always launched by clients, servers and clients in two-way Web service both have the ability to post a request and return a response [16]. In a two-way Web service, the client is required to expose an appropriate port for the server to correspond so that they can achieve a two-way interaction [11]. The interaction pattern of a two-way Web service is shown in Figure 1 below.
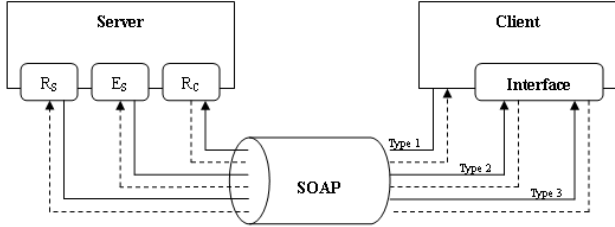

Figure 1.   Interaction pattern of Two-way Web service

In Figure 1, initial messages are indicated by the solid arrows and optional response messages are represented by the dotted arrows [11] and the meanings of R_C, E_S and R_S are given in the following:

- R_C: Initial Request from the client.
- E_S: Event reported by the server.
- R_S: Request arisen by the server.

Type 1 pattern presents the interaction of conventional one-way Web service between server and client [16]. The interaction pattern interpreted by Type 2 shows that the server issues the event notification and asynchronous reply to the client [16]. Type 3 describes the interaction pattern in which the server posts the service request to the client [16]. However, there are three "critical Web service methods" [11] which are necessary for implementing two-way Web services. They are WS-Addressing [5], WS-Session [1] and WS-Eventing [3].

B.   Overview of WSLU Architecture

In this article, we propose a WSLU to integrate authentication services with RFID-based authentication units seamlessly. The WSLU is constructed using the above infrastructures including UDDI, WSDL, SOAP, WS-Addressing, WS-Session and WS-Eventing. It is consisted of an administrator, a Web service locating server, a Web service synchronizer, a Web service database and an authentication unit database. The interactions between administrator, Web service locating server and Web service synchronizer are relied on SOAP message. WSLU can achieve effective system load balance and assign the authentication services for every RFID-based authentication unit according to its demand. Figure 2 presents the architecture of WSLU. We discuss each component in the architecture and its functionality as follows.
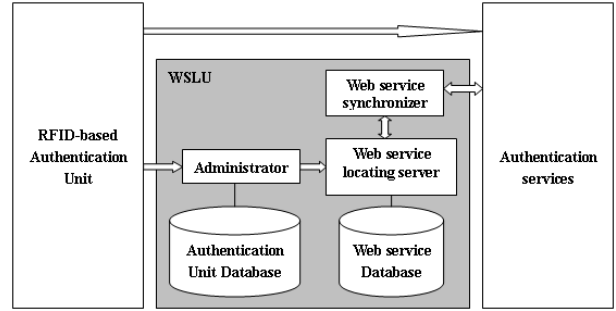

Figure 2.   Architecture of WSLU

- **Administrator:** When an authentication unit submits an authentication request, the request will be firstly sent to the administrator who analyzes this request immediately. After matching the identity information of the authentication unit with the records in authentication database, the administrator will abandon the request from illegal authentication units and transfer the legal request to the Web service locating server. Finally, the administrator will pass the searching result to the authentication unit.

- **Web service locating server:** According to the request, the Web service locating server searches for the most appropriate Web service from the Web service database and assigns the service to the authentication unit, and then returns the searching result to the administrator. In addition, the Web service locating server will alter the related record in the Web service database when receiving a message from the Web service synchronizer about the change of a specified Web service. Moreover, the Web service locating server will notify its change to the Web service synchronizer. (two-way web services)

- **Web service synchronizer:** As a broker between the authentication services and the Web service locating server, the Web service synchronizer subscribes the services information (including abstracts, interface and location information) of the authentication services. When receiving a notification of updating from an authentication service, the Web service synchronizer notifies the Web service locating server to renew the information about the relative authentication service stored in the Web service database. On the other hand, pushing a modification message to all authentication services and keeping the communication tunnel between the WSLU and the authentication services alive.

- **Authentication unit database:** It is used to store the identity information of each acknowledged RFID-based authentication unit which used for proving the validity of authentication unit.

- **Web service database:** The updated information of each authentication service is recorded in Web service database. For all the authentication requests, the Web service locating server will respond with

the most appropriate authentication service which is stored in the Web service database.

WSLU is managed by a third party organization that has the authentication to ensure the information stored in the databases is valid and trustworthy. Every authentication service provider should register its valid identification information to the third party organization, and it will receive a secret key to encrypt and decrypt the message exchanging with the WSLU. Thus, the scheme makes sure that authentication services can be trusted. Similarly, every RFID reader has to be registered in the third party organization. When an end-user of a RFID-based authentication unit makes a request for verifying a product with a RFID reader, he or she needs to offer an account to access authentication services. The account is maintained and verified by the third party organization too.

Additionally, the authentication services, the Web service locating server and the Web services synchronizer in the WSLU model are all with two-way Web services. Two-way Web service can help system always keep active, so end-users can enjoy an effective and reliable authentication service.

IV. RFID-CENTRIC ANTI-COUNTERFEIT SYSTEM

RFID-centric anti-counterfeit system [15, 20], an innovative authentication scheme, has emerged in recent years, and it is enjoying a close attention in industries and academic communities. Compared with traditional anti-counterfeit systems, the outstanding properties (large data capacity, unique ID, data encryption and ubiquitous network access) of RFID-centric anti-counterfeit system facilitate the development of anti-counterfeit technologies. In this section, we will present a RFID-centric anti-counterfeit system and discuss related concepts.

A. Basic Concept of Generic RFID System

A generic RFID system is consisted of three components as shown in Figure 3, namely **RFID Tag**, **RFID Reader** and **Backstage Computer** [13, 18].
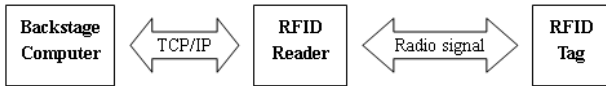

Figure 3. Components of RFID

In a RFID system, the data exchange between RFID tag and RFID reader is through radio signal within a near field. The data collected by reader is processed and calculated in backstage computer. However, we need some additional mechanisms for ensuring the security of data exchange between tag and reader. Two-way authentication, XOR operation and hash function, for instant, are utilized to guarantee the data security, which have been analyzed in [18]. In this article, we assume that all RFID systems have already considered the security issues mentioned above and implemented the relative security mechanisms. Therefore, the anti-counterfeit System we discuss here is in a secure RFID environment.

B. Architecture of RFID-centric Anti-counterfeit System

The authentication solution that we propose here is RFID-based online verification system which combines the advantages of RFID technology, Internet and wireless communication network. End-user can access the authentication services through various devices such as computer, PDA and Smart Phone, and the user receives the result from a given authentication service assigned by the WSLU according to an unique identical code captured from a RFID tag. On the other hand, due to the benefit from the Hitachi μ-chip technology [19] introduced into the RFID-centric anti-counterfeit system, we do not have to consider the counterfeit of the RFID tag in our scheme. The architecture of RFID-centric anti-counterfeit system is shown in Figure 4.
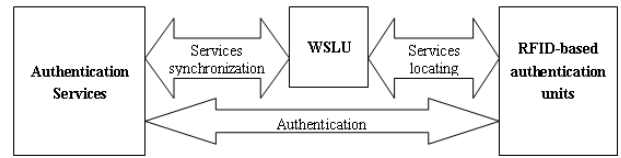

Figure 4. Architecture of RFID-centric anti-counterfeit system

- **Authentication services:** Authentication service providers may expose one or some authentication service(s) to WSLU via the authentication service synchronizer (a two-way Web service) in WSLU, and operates one or more authentication services interface(s) (one-way Web service(s)) to receive authentication requests from RFID-based authentication units. Each request is processed by backstage authentication components in the providers' servers, and the result is returned to RFID-based authentication units through authentication service interfaces.

- **WSLU:** WSLU is a Web services middleware which is critical to integrate authentication services with RFID-based authentication units seamlessly. It verifies the identity of each RFID-based authentication unit and assigns the most appropriate authentication service to it. Meanwhile, WSLU keeps updated information of all authentication services in its Web service (authentication service) database. This centralized management mechanism (including access control, service locating as well as user and service information management) reduces the complexity of RFID-centric anti-counterfeit system and prevents service hot spot.

- **RFID-based authentication unit:** As the user interface of RFID-centric anti-counterfeit system, RFID-based authentication unit could be any computer, PDA or Smart phone with the ability to access Internet and to correspond with RFID reader. In order to invoke an authentication service, it must have legal identity acknowledged by WSLU.

Therefore, when an end-user execute a verification he/she has to use a RFID reader connected to get the RFID

code from the object, and then a RFID-based authentication unit sends an authentication request with its identity information and the RFID code received from RFID reader to a WSLU. If the RFID-based authentication unit is acknowledged, it will be assigned to an authentication system to process the verification. Then, the authentication system responds with a verification result to the legal RFID-based authentication unit which displays the result to the end-user.

V. ARCHITECTURAL OUTCOMES

As the above mention, the WSLU is the most essential component in RFID-centric anti-counterfeit system not only due to its position in the system but also its functionality. The WSLU is a bridge connecting RFID-based authentication unit and authentication services, the authentication unit must be able to get a specified authentication service from the WSLU so that it could have the right to verify an object. If the WSLU is broken down or the authentication unit is illegal, the authentication process will be halted immediately. Additionally, the proposed architecture of RFID-centric anti-counterfeit system establishing a security mechanism to prevent authentication services from unauthorized access which may damage data integrity and cause data losing or disclosure. With the protection from the WSLU, the anti-counterfeit system can enjoy a high credibility and security. Moreover, the scalability has been enhanced after the WSLU was introduced because it is easier to add new authentication service or authentication unit to the existing anti-counterfeit system. Last but not least, the WSLU has an ability to reduce redundant data in the anti-counterfeit system because neither authentication service providers nor authentication units need to maintain the extra data such as identity information of authentication unit and the path information authentication service.

VI. EXPERIMENTS

We conducted several experiments and describe them in this section to determine the merits of the WSLU architecture. In the experiments, we first published five Web services, which represent the authentication services from three different companies for authenticating services. We assume that the authentication services WS_1 and WS_2, offered by Company A, are utilized for verifying two different products (P_1 and P_2). Company B provides another two authentication services (WS_3 and WS_4) running on two machines with different computing power for proofing the same product (P_3), and WS_3 has one time computing power more than WS_4. The last authentication service (WS_5) comes from company C, it can authenticate product P_4.

Additionally, we also provided another Web service (WS_WSLU) as the interface of the WSLU to respond the authentication requests from a RFID-based authentication unit and to assign the appropriate authentication service to the authentication unit. As the key component of the experiments, the WSLU has the knowledge of the RFID-based authentication unit and the authentication services.

In addition, an application (WA) played as a RFID-based authentication unit in our experiments. The RFID-based authentication unit has no knowledge about all the authentication services but the WSLU, thus it can focus on processing authentication requests rather than the redundant information from the authentication services. When processing an authentication request, the RFID-based authentication unit only needs to read the RFID tag ID from a product, and then convey the ID to the WSLU, which will assign the authentication service to the RFID-based authentication unit automatically. Lastly, the authentication unit can acquire the authentication result from the authentication service.

Here, we required the WA to send one thousand authentication requests for each product to the WS_WSLU randomly. Table 1 shows the experimental results.

TABLE I. EXPERIMENTAL RESULTS

Product	Authentication Services				
	WS_1	WS_2	WS_3	WS_4	WS_5
P_1	1000				
P_2		1000			
P_3			667	333	
P_4					1000
Total Access Times	1000	1000	667	333	1000

As Table 1 shows, the experimental data and our design are a perfect match. The one thousand authentication requests for the P_1 were all successfully located to its corresponding authentication service (WS_1) by the WS_WSLU, and the same results can also be found from the experiments of verifying the P_2 and P_4 which were assigned to the WS_2 and WS_5. In the case of P_3, the WS_WSLU located the one thousand authentication requests to the WS_3 and WS_4 based on their computing power. They were accessed 667 and 333 times respectively.

Thereby we can easily know that each authentication request is assigned to an appropriate authentication service, although the RFID-based authentication unit has no knowledge about the authentication services. Additionally, the RFID-based authentication unit can be released from maintaining the redundant authentication services information, and it does not have to worry about the change of authentication services. Furthermore, the WS_WSLU can achieve a good load balance of the services with different calculation power and thus the WSLU can simplify the deployment of RFID-centric anti-counterfeit system over the Internet

VII. CONCLUSION

In this paper, we have presented the WSLU (a two-way Web service-based solution of authentication services locating) which supports seamless services integration, access control, load balance and service notification. Its merits have been proved by our experiments in Section 6. With the contribution of WSLU, the RFID-centric anti-counterfeit system can provide an effective and secure authentication service. However, this approach only discusses the security and efficiency in software perspective and is based on the assumption that there is a sufficient

scheme for hardware security utilizing existing two-way authentication, XOR operation and hash function.

The security issues of the authentication data and the data transmission between the three components of RFID-centric anti-counterfeit system have been conducted to investigate in our future work.

REFERENCES

[1] WS-Session - Web Services for Application Session Services, 2008, http://www.ecma-international.org/publications/standards/Ecma-366.htm.

[2] SOAP Version 1.2, 2007, http://www.w3.org/TR/soap/.

[3] Web Services Eventing, 2006, http://www.w3.org/Submission/WS-Eventing/.

[4] Web Services Description Language (WSDL) for CSTA Phase III, 2006, http://www.ecma-international.org/publications/standards/Ecma-348.htm.

[5] Web Services Addressing 1.0 - Core, 2005, http://www.w3.org/TR/2005/CR-ws-addr-core-20050817/.

[6] Web Services Addressing (WS-Addressing), 2004, http://www.w3.org/Submission/ws-addressing/.

[7] Web Services Security, 2004, http://www.ibm.com/developerworks/library/specification/ws-secure/.

[8] RFC 2396, 1998, http://www.faqs.org/rfcs/rfc2396.html.

[9] UDDI Version 3 Features List, http://uddi.org/pubs/uddi_v3_features.htm.

[10] E. Christensen, F. Curbera, G. Meredith and S. Weerawarana, Web services description language (WSDL) 1.1, W3C note, 15, Mar. 2001, http://www.w3.org/TR/wsdl.

[11] Feng Liu, Gesan Wang, Li Li and Wu Chou, "Web Service for Distributed Communication Systems," Proc. IEEE Service Operations and Logistics, and Informatics (SOLI 06), IEEE Press, June 2006, pp. 1030-1035, doi: 10.1109/SOLI.2006.328893.

[12] Feng Liu, Gesan Wang, Wu Chou, L. Fazal and Li Li, "TARGET: Two-way Web Service Router Gateway," Proc. IEEE Web Services (ICWS 06), IEEE Press, Sept. 2006, pp. 629-636, doi: 10.1109/ICWS.2006.127.

[13] K. Finkenzeller, RFID Handbook : Fundamentals & Applications in Contactless Smart Cards & Identification, 2nd ed.Chichester: Wiley, 2002.

[14] Kuo-shien Huang and Shun-ming Tang, "A web services based framework for RFID bike rental business solutions," Proc. IEEE Industrial Engineering and Engineering Management, IEEM Press, Dec. 2008, pp. 1475-1479, doi: 10.1109/IEEM.2008.4738116.

[15] M. O. Lehtonen, F. Michahelles and E. Fleisch, "Trust and Security in RFID-Based Product Authentication Systems," Systems Journal, IEEE, vol. 1, Dec. 2007, pp. 129-144, doi: 10.1109/JSYST.2007.909820.

[16] L. Li and W. Chou, "Two-way Web service: from interface design to interface verification," Proc. IEEE Web Services (ICWS 2005), IEEE Press, July 2005, pp. 532, doi: 10.1109/ICWS.2005.124.

[17] Noh-sam Park and Gil-haeng Lee, "Agent-based Web services middleware," Proc. IEEE Global Telecommunications Conference (GLOBECOM '03), IEEE Press, Dec. 2003, pp. 3186-3190, doi: 10.1109/GLOCOM.2003.1258824.

[18] Yung-Chin Chen, Wei-Lin Wang and Min-Shiang Hwang, "RFID Authentication Protocol for Anti-Counterfeiting and Privacy Protection," Proc. Advanced Communication Technology (ICACT 2007) , Feb. 2007, pp. 255-259, doi: 10.1109/ICACT.2007.358350.

[19] R. Imura, "The Role of Networked RFID for Driving the Ubiquitous," Proc. IEEE Emerging Technologies and Factory Automation (ETFA 06), IEEE Press, Sept. 2006, pp. 1115-1118, doi: 10.1109/ETFA.2006.355250

[20] M. Potdar, E. Chang and V. Potdar, "Applications of RFID in Pharmaceutical Industry," Proc. IEEE Industrial Technology (ICIT 2006), Dec. 2006, IEEE Press, pp. 2860-2865, doi: 10.1109/ICIT.2006.372726.