2009 Second International Conference on Intelligent Computation Technology and Automation

# Wireless Food Ordering System Based on Web Services

XU Hongzhen, TANG Bin, SONG Wenlin
Department of Computer Science and Technology
East China Institute of Technology
Fuzhou, Jiangxi Province, 344000, China
xhz_97@163.com

*Abstract*—**Current wireless communications enable people to easily exchange information, while web services provide loosely-coupled and platform-independent ways of linking applications across the Internet or Intranet. This paper presents an integration of wireless communication technologies and web services technologies to realize a wireless food ordering system. In this system, it implements wired and wireless data access to the servers and food ordering functions through both desktop PCs and mobile devices such as PDAs over a wired/wireless integrated local area network. To sure the security of the system, the secure web service architecture and some security strategies to ensure mobile communication security are discussed. Web services-based wireless applications on mobile devices provide a means of convenience, improving efficiency and accuracy for restaurants by saving time, reducing human errors, etc.**

***Keywords Web Services; Wireless; Food Ordering System; security***

## I. INTRODUCTION

The rapid developments in information technology, particularly in wireless communication and web services technologies, are greatly changing the way people access and work with information. The convenience and powerful functionality offered by mobile devices such as PDAs, has encouraged many people to investigate the benefits of using them. Wireless and handheld devices abound as vendors pitch the common themes of one-to-one computing, instant communication and anytime, anywhere information access [1]. While web services provide a technology for service-oriented computing. Web services allow programs written in different languages on different platforms to communicate with each other in a standard way [2]. By integrating these technologies, consistent business models can be implemented on a broad array of devices: not just on mobile devices operating over mobile networks, but also on servers and PCs connected to the Internet.

The food ordering process in restaurants requires the coordination of simple tasks. Instruction flows mainly from customers to waiters then to kitchen and/or the bar staff, finally to the cashier [3]. In a medium to large and busy restaurant this coordination is a challenge and requires an efficient ordering system. Errors in ordering processes lead to incorrect or out of sequence meal preparation or non-consumable and results in added cost to the business.

This paper presents an integration of wireless communication technologies and web services technologies to realize a wireless food ordering system. In this system, it implements wired and wireless data access to the servers and food ordering functions through both desktop PCs and mobile devices such as PDAs over a wired/wireless integrated local area network. The system is based on secure web service architecture and some security strategies to ensure mobile communication security are adopted. Web services-based wireless applications on mobile devices provide a means of convenience, improving efficiency and accuracy.

## II. WIRELESS LAN AND WEB SERVICES

### *A. Wireless LAN*

A wireless LAN (WLAN, Wireless Local Area Network) is a flexible data communication system implemented as an extension to or as an alternative for, a wired LAN within a building or campus [4]. Using electromagnetic waves, WLANs transmit and receive data over the air, minimizing the need for wired connections. Thus, WLANs combine data connectivity with user mobility, and, through simplified configuration, enable movable LANs.

The IEEE 802.11 group of standards specifies the technologies for wireless LANs. 802.11 standards use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing and include an encryption method, the Wired Equivalent Privacy algorithm. The 802.11a, b, and g standards are the most common for home wireless access points and large business wireless systems.

A remote user can use WLAN to access the Internet through public access points (“hotspots”) provided by service providers. When in the office, they may access WLAN through wireless access points. In enterprise environments, WLANs are usually complemented by security mechanisms, such as VPN (Virtual Private Network).

Over the last several years, WLANs have gained strong popularity in some markets, including the health-care, retail, manufacturing, and academic areas. These industries have profited from the productivity gains of using hand-held terminals and notebook computers to transmit real-time information to centralized hosts for processing. Today WLANs are becoming more widely recognized as a general-

978-0-7695-3804-4/09 $26.00 © 2009 IEEE
DOI 10.1109/ICICTA.2009.830

purpose connectivity alternative for a broad range of business customers.

### B. *Web Services*

Quickly becoming a significant technology in the evolution of the Internet is web services, a set of standards that can interconnect systems over a verity of networks. It is an open XML-based technology providing a generic data exchange format and has been rapidly adopted by many vendors. Web services can easily be built upon existing applications, no matter what the underlying technology is. Because they are expected to have a growing familiarity and acceptance among many users and offer great technological promises, Web services are an interesting subject for the investigation of their possible application in many systems [5].

Web services are a new generation of web application. It combines the advantages of the component-oriented methods and web techniques, and they can describe its own service. It can also publish, locate and transfer modularized application in web. The provided functions of web services may be simple, but it also contains extraordinary complicated business logic. Web services represent a kind of implementation of SOA (Service-Oriented Architecture), and they are the most popular one. In addition, the three operations of SOA can only process when the components of SOA interact. Therefore some standardized techniques are used in web services, including UDDI, WSDL, HTTP, SOAP, and XML and so on. Web services become the best choice for developing application of SOA [6].

## III. Design and Implementation of the System

### A. *System Architecture*

In the system, we adopt four-tiered web-based client-server architecture. Figure 1 shows the overview of the system architecture. The system is conceptually composed of six main components: the web server, database server, cash register, mobile context server, mobile user and desktop user. The web server provided relevant information for mobile devices or desktop PCs on a wired/wireless integrated local area network using WSDL (Web Service Description Language) to describe functions and protocols. The web server then transmits to the mobile devices or desktop PCs. The user binds the web server and the WSDL. This enables the web service to be used by correspondence using SOAP (Simple Object Access Protocol). The database server saves all information of the system such as food information, ordering information, client information. The cash register is responsible for cost calculation of the consumer. The mobile context server applies context to the contents by using styles, an attribute override, and templates according to the resources of a given mobile device.

Desktop users can ask for services after checking the WSDL of the service from the web server. A desktop on a wired network can be used to browse full contents on one screen shot. When a user requests food information through a wired network, the web server serves the information by connecting to the database server. When a user requests food information through a wireless network, the mobile context server divides the context pages according to the screen size of the mobile device. It also filters the pages according to mobile devices and then browses the adopted content from the context server to the mobile web browser. The mobile context server reconfigures contents offered by the web server.

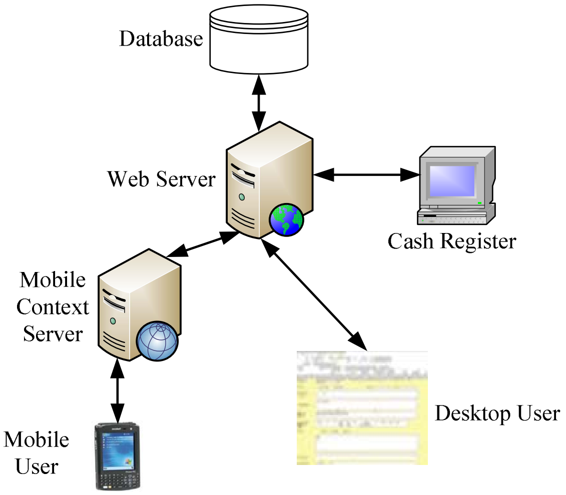

Figure 1. The System Architecture

### B. *Web Service Security Model*

Web service security can be applied at three levels [7]:

- Platform/transport-level (point-to-point) security;
- Application-level (customer) security;
- Message-level (end-to-end) security.

Each approach has different strengths and weaknesses. The choice of the approach is largely dependent on the characteristics of the architecture and platforms involved in the message exchange. This system focuses on platform- and application-level security, so the two security levels are described.

#### *1. Platform/transport-level (point-to-point) security*

The transport channel between two endpoints (web service client and web service) can be used to provide point-to-point security as illustrated in Figure 2.

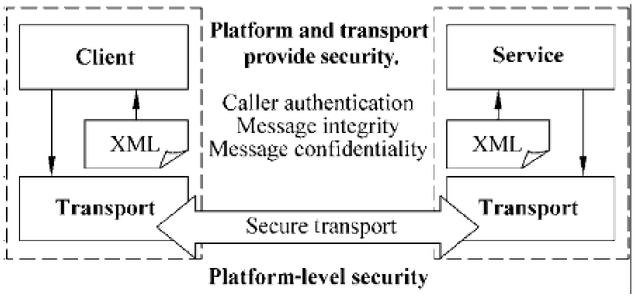

Figure 2. Platform/transport-level security

In the platform-level model, the client sends an XML format request to the web server. The XML message is not encrypted by the client. When the message is transported in the transport channel, the network encrypts the entire data stream to make sure that the transport is secure.

This system uses a tightly coupled Microsoft Windows operating system environment. The Internet Information Server (IIS) provides basic, integrated and certificate authentication. The ASP.NET web service inherits some of the ASP.NET authentication and authorization features. The Secure Sockets Layer (SSL) is used to provide message integrity and confidentiality.

*2 Application-level security*

With application-level security, the application controls security with custom security features (Figure 3).

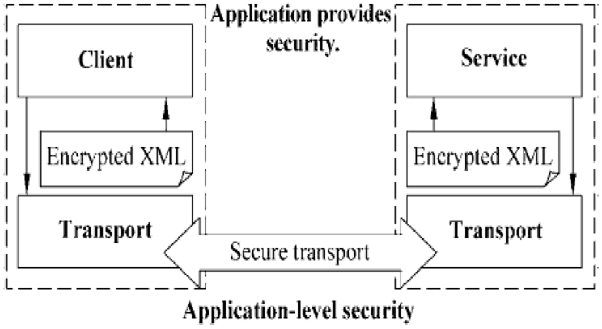

Figure 3. Application-level security

In the application-level security model, for example, an application can use a custom SOAP header to pass user credentials to authenticate the user with each web service request. A common approach is to pass a ticket (or user name or license) in the SOAP header. The application has the flexibility to generate its own principal object that contains roles. The application can optionally encrypt what it needs to, although this requires secure key storage and developers must have knowledge of the relevant cryptography APIs. An alternative technique uses SSL to provide confidentiality and integrity it with custom SOAP headers to perform authentication.

The system uses the SOAP Toolkit 2.0[8, 9] offered by Microsoft, which provides support for internet security based on the IIS security infrastructure to implement the application-level security model.

## C. *The Implementation of the System*

The whole system was built using the Microsoft .NET framework and .NET compact framework. Server application was implemented by Microsoft ASP.NET based on C#, the database was served by Microsoft SQL server 2000. The context server connected to the web server acted as IIS as the web server.

The function modules of this system mainly consist of 5 parts: system management, food management, client management, food ordering management and finance management, as shown in Figure 4.

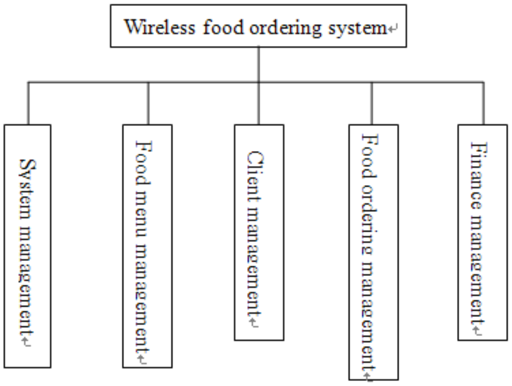

Figure 4. function modules of the system

The system management module is responsible for the initial setting of the system, administrator setting, wireless network setting, logs management etc. The food menu management includes setting name, prides, types, state of food, and so on. The client management supervises information of clients, which include the VIP information. The food ordering management is responsible for supervising the food ordering information from wire users and wireless users. The finance management administrates cash, bill, and financial audit of the restaurant. Some user interfaces of wire users and wireless users in this system are shown in figure 5 and figure 6.

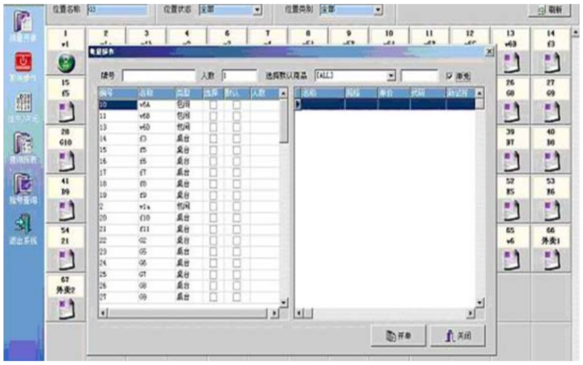

Figure 5. A view of desktop PC

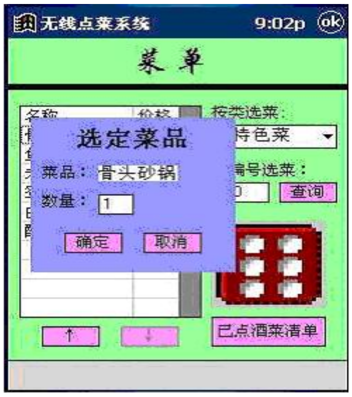

Figure 6. A view of PDA

### D. Security strategies with mobile devices

Secure wireless connectivity between mobile terminal devices and the web server is an important aspect of this system. Some of the specific security threats associated with mobile devices include [10]:

- Interception of data that passes over the wireless network
- Capture of data via wireless connections
- Mobile viruses

So the web services-based wireless food ordering system should be provided efficiently with a high level of security. In this system, we adopted the following strategies to ensure mobile security:

- The critical data are not stored permanently in the device. The application will delete data downloaded from the database before the mobile terminal is closed.
- Encryption. We use the WLAN encryption standard WEP (Wired Equivalence Privacy) to encrypt the data in transit.
- Individual authentication. The critical software on the system needs a username and password for use to implement individual authentication.
- MAC address filters. A MAC (Media Access Control) address is a unique identity burned into every network adapter during manufacture, with no way of changing it. Using this filter, the AP (Access Point) maintains a list of MAC addresses of mobile devices of the restaurant and only permits those devices on the list to connect to the server.

## IV. Conclusions

The mobile devices have been widely used to provide easily access to the web content. We presented a wireless food ordering system based on web services over a wired/wireless integrated local area network, which implements wired and wireless data access to the servers and food ordering functions through both desktop PCs and mobile devices such as PDAs. The system is based on secure web service architecture and can increase efficiency for restaurants by saving time, reducing human errors and by providing higher quality customer service.

## Acknowledgment

The authors wish to thank the support by the Scientific Research Plan Projects of Jiangxi Education Department (No. GJJ09263) and the Jiangxi Province Natural Science Foundation (2007GZS0472)

## References

[1] C. Branigan (2001), Wireless, handheld solutions prevail at NECC 2001, retrieved January 10, 2007 from http://www.eschoolnews.com/news/showStory.cfm?ArticleID=2865.

[2] Watkins Demien. Mobile web services technical roadmap. http://www.microsoft.com/serviceproviders/mobilewebservices/mws_tech_roadmap.asp. 2003, 11.

[3] Y. Xiang, W. Zhou and M. Chowdhury. Toward pervasive computing in restaurant, First International Conference on E-Business and Telecommunication Networks (ICETE 2004), Setubal, Portugal, August, 2004, pp312-317.

[4] IEEE 802.11$^{TM}$ WIRELESS LOCAL AREA NETWORKS. IEEE Working Group (WG), http://www.ieee802.org/11.

[5] Knikker, R., Guo, Y., Li, J.L., Albert Kwan, K.H., Yip, K.Y., Cheung, D.W., et al..A Web services choreography scenario for interoperating bioinformatics applications. BMC Bioinformatics 2004, 5:25-28.

[6] FENSEL D, BUSSLER C. The Web service modeling framework WSMF. Electric Commerce Research and Application,2002, Vol.1,No.2:pp113-137.

[7] Meier J D, Mackman A, Dunner M, Vasireddy S. Web services security S. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/SecNetch10.asp.2002.

[8] Powell Matt. Real SOAP security. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnservice/html/service11212001.asp. 2001.

[9] Kirtland Mary. Secure web services using the SOAP toolkit. http://msdn.microsoft.com/archive/default. asp?url=/archive/en-us/dnarxml/html/websvcs_usingsoap.asp. 2001.

[10] R. G. Duncan and M.M. Shabot "Secure remote access to a clinical data repository using a wireless personal digital assistant (PDA)" . Proceedings of the American Medical Informatics Association Symposium, 2000, pp210-214.