MWALLET: A Mobile based E-Ticketing System with Push Technology

Balaji TK
Post Graduate student, Department of CSE
Sri Venkatesa Perumal College of Engg. & Tech.,
Puttur, Andhra Pradesh, India.
balajitk7@gmail.com

Janardhan Babu V
Professor, Department of CSE
Sri Venkatesa Perumal College of Engg. & Tech.,
Puttur, Andhra Pradesh, India
cse.svpacet@gmail.com

Abstract—The World Wide Web provides an information delivery infrastructure for various types of digital contents used in daily life. Payment infrastructures such as digital cash, micropayments, and encrypted credit cards have also been established. However, no digital medium or infrastructure that prevents duplicate redemption and enables the trading of various rights, much like paper tickets, has been established yet. We are thus developing a generalized digital ticket system that can circulate any type of rights. A digital ticket is a digital medium that guarantees certain rights of the ticket owner and it includes software licenses, resource access tickets, event tickets, plane tickets, etc. In this paper I propose a prepaid smart metering scheme for Smart Grid application based on centralized authentication and charging using the WiMAX prepaid accounting model with push technology as an enhancement and providing more security with flash based 2D color barcode.

Keywords-Smart payment; Demand Response; push technology; digital tickets; QR-code;

I. INTRODUCTION

As the Indian economies develop and the 3G eracomess popular, E-ticketing has shown a broad future. On the one hand, E-ticketing is of great advantages. Compared with traditional way of ticketing, e-ticketing is convenient, safe and of low-cost. What’s more, it can extend value-added services such as WAP service and provide personnel services since it can count and manage tickets automatically and accurately [1,2]. As a consequence, although still in its infancy, e-ticketing has great market potential and already launched applications in some areas. So, all the parties on the industry chain, such as telecom operators, software providers, terminal manufacturers, banks, are trying hard to occupy the market. However, there still exist some serious problems

Industry chain need to be developed: lots of parties are involved in mobile ticketing, and they compete with each other as well as cooperate: the financial institutions will get some share of the profits from every closed deal since it assumes the account management of the ticket-sellers and buyers; the mobile network operators will charge the service providers, some fee since they provide safe communicating channel for the payment and earn some value-added profits; the mobile payment party will charge the mobile operators and financial institutions for the permission of using payment techniques; the sellers expect to abridge the processes so that the expenses can be cut down while the customers care about the safety and convenience. Consequently, it remains a big problem how to balance the interests of so many parties and integrate various resources in order to get a win-win situation.

Lacking a universal mobile ticketing system: to accomplish one kind of e-ticketing is not hard at all, and I can find many successful cases both outside and inside China, but what’s hard is to integrate all kinds of ticketing, such as cinema entrance tickets and transportation tickets, into one system and apply it into one mobile phone, in order to get a universal, security and long term mobile ticketing system. For the reason that each type of tickets has different characteristics and they are sold in various ways and involve enormous number of participants.

Other problems: firstly, current ticketing systems cannot support refund and exchange tickets automatically without mankind operation. Secondly, it still needs to print out the ticket when checking in, thus there is no real sense of electronic management and operations. Besides, the security and confidentiality of mobile payments need to be enhanced. As for all the problems mentioned above, this paper introduces a third party universal mobile e-ticket system, called Mobile WALLET (MWALLET). MWALLET is an integrated ticket platform that can solve the problems mentioned above. Firstly, it requires every participants conform to the same principles made by the trusted authority, which defines the dividing of the profits and allows conciliation if disagreements arise. Finally, it introduces a new kind of electronic receipt, dynamic two dimensional barcode, to help to enhance the security of the payment and can replace the traditional paper tickets. MWALLET is composed of universal mobile ticket platform and external supporting environments [5]. The platform provides interfaces for both individual user clients and enterprise user clients. Hence, it can provide high quality services of can provide high-quality services of both ticket booking and non-ticket reservations such as hotel reservations. And external supporting environments include users’ mobile phones, computers, payment platform, and current enterprises’ ticketing systems and financial institutions such as banks and certificate authorities. More over we are using Mobile Push uses SMS and HTTP technology for delivery, which makes it suitable for applications where it is important to ensure that the latest information is always available at the receiving end, without the need to frequently poll for updates. As long as the phones you want to push the content to have your push-
enabled Android or Java ME application installed, you can rest assured that your content will be received instantly.

II. THE GENERAL FRAMEWORK AND THE FUNCTIONS OF MWALLET

The purpose of designing MWALLET is to provide secure online service of inquiry, booking, payment and refund, a universal mobile ticketing platform which can be used to report false information, to facilitate the reunification and regulation of the various ticketing providers, to promote healthy competition in order to achieve a win-win situation, and to record users’ ticketing history in order to provide targeted service and thus make value-added profits for merchants.

A. The Framework of MWALLET

MWALLET is composed of four major parts: universal third party mobile ticketing platform (MWALLET platform), payment platform, checking system and existing businesses’ ticketing systems. And the MWALLET platform is the very crucial part that provides interfaces for the other three and coordinates the operations of the whole system. And the components of MWALLET platform will be discussed in section 3 Maintaining the Integrity of the Specifications.

B. The Flowchart for Customers to Function The System

The flowchart for customers to function the system is as follows: Enterprise users release and manage ticket information through their current management systems or the enterprise user end offered by the system.

Personal users login the system and then do businesses such as inquiry and booking, and then submit the ticket information to the merchants.

Personal users use the third party payment system as business agency and remit money to its account. And when the user registers, he must provide valid certificate that can show his real identification, so that the security of this system is improved.

III. THE COMPONENTS OF MWALLET PLATFORM AND ARCHITECTURE

The MWALLET platform is composed of ticket system, refund system, member management system and micro clients running on users’ phones and enterprises’ computers. And it also provides interfaces to existing businesses’ ticketing systems [7].

A. Ticketing System Based on B/S Architecture

Enterpriser users publish and manage ticket information by web sites. Individual users make the associated ticketing inquiries and reservations through the mobile phone WAP network and complete online payment through mobile phones banking or other mobile payment methods. After the success of booking, individual users will get an order number. And then the order number will be delivered to personal user’s client to generate corresponding 2-D barcode image.

B. E-ticket Management System Based on C/S Architecture

The client end of E-ticket management system runs on the individual’s mobile phone. And its functions include managing order number, communicating digital signature with the server and generate 2-D barcode image. Manage order number: capture order number from wap, classify and preserve order number, dispose overdue order number. And in order to ensure the security of e-tickets, must add digital signature when the client end transform order number into 2-D barcode image [8]. And the process of generating 2-D barcode image will be discussed in section 4.2 since it adopted a security mechanism. units.

C. The Chosen of Mobile Payment Method

There are three kinds of mobile payment methods [9,10]. The first method is that the users pay the cost of mobile ticketing at the same time with paying their mobile bills. That is, the mobile network operators charge the bills and later pay the money to the merchants. But this approach is within very limited scope of businesses and can handle only a small sum of money due to the reason that the network operators are not financial institutions and hence cannot do banking business. So this method cannot be applied in mobile ticketing. The second method is based on the banks. Usually, the users need to go to the mobile business hall with their identity certificate to get special SIM card, and then login the mobile website to recharge for the mobile wallet using credit card. But this method has disadvantages: A mobile phone can only be combined with one or a few banks, not convenient for users; different banks cannot interact with each other, limiting the promotion of mobile payment; every bank need to purchase their own equipment, a waste of resources. And the third is what is adopted in MWALLET, called third party payment method. Third party payment refers to the kind of online payment mode that an independent body of a good reputation signs with the major banks, and then provides interfaces to bank payment system in order to accomplish payment. In third party payment, the customers choose what they need and then use third party payment platform to pay. Then the third party notifies the sellers that the payment is credited into account and asks for goods delivery. After the customers receiving the goods and making confirmation, the third party will give the money to the sellers’ account. So the third party plays the role as the connection between the sellers and the banks and the online supervisor. And it can coordinate all the processes of the transaction, charge for the ticket information release, operate and maintain the platform and collect users’ ticketing information. Thus it waives the disadvantages of the former two methods.

D. Check and Refund Ticket System Based on B/S Architecture

When checking the tickets, the first thing is to decode the 2-D barcode and then search the database to judge whether the e-ticket is valid. It will only pass through when it is valid. And when the customer wants to refund, he just need to login the system and request for refund and after confirmation, the system will change the database, and the e-ticket will be listed invalid and the customer will get the money back from the third party, and then the third party will ask the money back from the customer.
E. Architecture of MWALLET

Our MWALLET is designed to support the goals all of us. Figure 1 shows Brief descriptions of the MWALLET Architecture functions:

1. The Instrument Manager manages the entire instrument instances contained in the wallet, and, for example, may be queried to determine which instrument classes and instances are available to execute a given payment or other operation.

2. The Protocol Manager manages all of the protocols that the wallet may use to accomplish various operations, and invokes protocols to carry out the interaction between the MWALLETand the vendors and banks. The Protocol Manager relies on the communication manager to process low-level communications requests with other computers representing banks and vendors.

3. The Wallet Controller presents a consolidated interface for the wallet to the client. The Wallet Controller hides the complexity of the other components of the wallet, and provides a high-level interface to the client. A non-human client, or software agent, can make method calls on the Wallet Controllers interface through the Client API. A human client may use a graphical user interface (GUI) which may make method calls on the Wallet Controller. The Wallet Controller coordinates the series of interactions between the User Profile Manager, Instrument manager, and Protocol Manager necessary to carry out high-level requests received from the client, such as purchase a product.

4. The User Profile Manager manages information about clients and groups of clients of the wallet including their user names, passwords, ship-to and bill-to addresses, and potentially other user profile information as well. In addition, the User Profile Manager keeps access control information about what financial instruments each user has the authority to access.

5. The Communication Manager provides the wallet with an interface to send and receive string messages between wallets and peer commerce components by setting up a connection with a remote Communication Manager. The Protocol Manager builds on top of the connection abstraction to support the concept of a session. A connection is typically asynchronous, while communications between peer commerce components in a Session occur in (message, response) pairs where one peer sends a message; the other peer receives the message, executes some action, and returns a response. Depending upon the implementation of the Communication Manager, the messages may be sent over different types of networks using different communication protocols. For example, send and receive messages over the Internet using HTTP requests and responses over a TCP/IP Ethernet network. In this case, a Session may be made up of a sequence of several HTTP GET messages and their corresponding responses. Note that the Protocol Manager is responsible for making calls to the Cryptographic Engine to encrypt any data that is passed to the communication manager, such that the data can be securely transmitted over the communications medium. The Communication Manager cannot be responsible for encryption of sensitive data from the wallet because it is formally outside the wallet architecture, and can be replaced by another communication manager to run the wallet on another device. If the communication manager is relied to encrypt sensitive data then the communication manager might be replaced with a malicious Communication Manager that sends all sensitive data to an adversary.

6. The Client API is an interface provided by the Wallet Controller that may be used by an autonomous software agent acting on behalf of a human user.

7. The User Interface provides a graphical interface to the services offered by the Wallet Controllers interface. The User Interface is an optional component of the wallet. Some devices, such as most smart cards, do not have the ability to display a graphical user interface, and hence the Wallet Controller interface must be accessed through the Client API. Note that the user interface is a core component within the wallet because certain parts of the user interface have access to sensitive user data. For example, the edit box object into which a user enters the password to unlock the wallet should run within the wallets protected address space. On the other hand, users may want to customize the wallets interface by plugging-in GUIs developed by other software vendors. To accomplish both these conflicting goals, the user interface exports parts of its interface as the User Interface API that may be overloaded by software vendors to render customized parts of the interface.

IV. WHAT GUARANTEE THE SECURITY OF MWALLET?

Security is a key issue. So in this part, I will discuss the e-receipt and encryption algorithms and other techniques that used to ensure the security of MWALLET.

A. Dynamic 2-D Barcode as a Security E-receipt

2-D barcode uses specific geometry to record data by a certain law of distribution of black and white graphic, read through image input device or electro-optical scanning device automatically so as to achieve automatic processing of information. It has some traits similar to barcode, but it can deliver information both horizontally and vertically thus
can deliver large sum of information in a tiny area [11]. 2-D barcode has the features of large capacity, high-quality of decoding, and strong security compared to barcode. Besides, the information carried can be restored even if it tears up or is contaminated, obviously superior to barcode. Ticket can be identified by special identifiers. While in 3G era, people are more likely to use mobile phones to get more information about various products, so they seek to identify 2-D barcode that contains the information of certain products actively with their own mobile phones. Thus 2-D barcode can be very level phones may be unable to satisfy the users’ complicated as it contains more information [13]. As a result, current identifying techniques and lower-needs. And another problem is the security of the 2-D barcode when it is used as an e receipt cannot be guaranteed, because it can be easily taken a picture of by another person and thus used unlawful by the person.

In order to solve the capacity problem mentioned above, people are trying to create a new type of 2-D barcode such as colored barcode that use colors to contain additional information. But it leads to new problems: color distortion on some screens may cause the failure of identifying; and as a newly-born barcode, it has many different types without an official type, which hampers the application of it. Besides, it cannot solve the security problem mentioned above. Since traditional 2-D barcode adopted an encryption technique, it can only be read by special tools which are facilitated with decryption algorithms. As a result, it ensures the privacy protection of the merchants and users and enhances the security. However, the security of the pictures themselves is usually ignored. For example, the 2-D barcode saved in a mobile phone can be easily taken a picture of and then be used by somebody else. In order to solve all the problems mentioned, we created a new type of dynamic 2-D barcode that combine the advantages of traditional 2-D barcode and colored barcode. It is a tiny flash composed of several traditional 2-D barcodes that appear, alternately, which cannot be taken picture of and can increase the capacity by several times without making it more complicated. In this way, we can use current coding and decoding algorithms of 2-D barcode with just a little change. And since it is dynamically changing, it cannot be taken a Picture of, thus ensure the security of the picture itself. Therefore, we apply this kind of 2-D barcode as an E-receipt to MWALLET.

B. MD5 Applied to the Database Management and Ticket Management

MD5 is a widely used encryption algorithm. It can transform a passage of message into a piece of 128 bit message-digest and can hardly be transformed back from message-digest back to the original message. So even if the message-digest is let out, the real message still remains unknown. So some sensitive data such as users’ passwords will be encrypted by MD5 and then be saved as message digest in the database. Therefore, the next time the user check in, the system will transform the new input data into message digest and then compare it with the one that saved in the database in order to judge whether the user is legal. In this case, even if the database manager will never know the user’s password, ensuring the security of such sensitive data. In order to ensure the security of e-tickets, I must add digital signature when the client end transform order number into 2-D barcode image. The processes are as follows:

The client end generates a string “S” (digital signature) randomly;

Using MD5 to transform S into “M” and then send it to the server side;

The server then saves “M” in corresponding database;

The client end will incorporate order number and “S” Generating 2-D barcode image: As noted above, the client end incorporates the order number and “S” into 2-D barcode image. While validating 2-D barcode, the validating system must first read out “S” from 2-D barcode image and then use MD5 to transform “S”, and compare the transformed value with “M” stored in database, only if they are the same will it be allowed to enter the next operating step. One-way nature of MD5 algorithm assures that “M” leakage will not lead to “S” leakage, thus ensuring the security of 2-D barcode.

C. MWALLET using PUSH Technology

Push, or server push, describes a style of Internet based communication where the request for a given transaction is initiated by the publisher or central server. It is contrasted with pull, where the request for the transmission of information is initiated by the receiver or client with Pull or Pull. Pull technology is based on the traditional request-reply model. It requires that users know a priori where and when to look for data. It suffers from transmission latency and duplicate data traffic.

Push technology allows users to get information as soon as it become available and users do not have any knowledge about virtual information servers. This transfer of control from users to providers is a potential problem. Focus is on Multicast-base push protocols. Push methods may be used by organizations to distribute information on their own “intranets” as well as by individual users who have placed the appropriate software on their own PCs in order to have information pushed from the Internet. That is, the technology may be used in diverse settings and in varying ways.

The above diagram shows that the push technology is involving to multicast the new applications or any new information about the MWALLET that are added to the

![Figure 2. Push technology](image-url)
framework by the enterprisers using AMP or CMP. CMP - Cyclically deliver a site’s most frequently changing and heavily requested documents on the same multicast address. Based on raw IP multicasting. Reliability is basically achieved through simply repetitive, cyclic transmissions.

D. Other Adoptions that Ensure the Security

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled. Payment is a great concern of both the sellers and the buyers. As is discussed in 3.3, the third party payment method adopted in MWALLET hides the information of users’ credit cards from public and therefore cut down the chance of the information being stolen and the combination of B/S and C/S architecture, discussed in section 3, achieves not only the distribution of the system but also the load balance. Therefore, it improves the stability and security of the database.

As is shown in this set of figures, Figure 3 is what MWALLET looks like in the mobile phone, and after clicking on the icon then comes all kinds of tickets and related value added services. And when choosing the movie icon, I can follow and Figure 4 is the payment page. Lastly, Figure 5 shows the dynamic 2-D barcode as a security e-receipt.

V. A Case Study of the System

As is discussed in section 1, MWALLET has overcome some weaknesses of exiting ticketing systems, bringing great convenience to the users and achieving win-win situation. And it uses dynamic 2-D barcode, which is proposed for the first time ever as a e-receipt which concentrates on not only the security of the information hidden in the barcode but also the security of the picture itself. Also, the architecture of MWALLET is smart because it combines C/S and B/S wisely.

It runs the encryption and decryption and some other functions that require great resources on the client end (C/S), and ticketing, check-in and refund functions which need to access may seem just as normal as other ticketing systems but it greatly improves the efficiency and the security.

We had free Android version tools to generate the QR-code with ports to other languages. Our focus is on using the built-in camera on mobile phones to scan and decode barcodes on the device, without communicating with a server.

VI. Future Work

Everything that made by the mobile is shown in the figure (anticipated future). This is what we do with single finger tip as an event ticket, print from camera by holding it close to printer, share business cards with a touch, pay for your goods with a tap of your phone, get on the bus bus waving your phone, setup your wireless home office with a touch and get information by touching smart poster.

Figure 3. MWALLET icon

VII. Conclusion

As the mobile commerce develops, the requirements of both the customers and the enterprises are changing rapidly. And a third party universal mobile ticketing system is needed to better satisfy the needs. MWALLET comes out just in time. Besides, it uses a new dynamic 2-D barcode which has much larger capacity and can guarantee the security when it is served as an e-receipt. As a consequence, MWALLET shows a broad future.
REFERENCES


