Construction of a Real-Time and Secure Mobile Ticket System

CHIN-LING CHEN[1], YEONG-LIN LAI[2], CHIH-CHENG CHEN[2] AND KUN-CHIH CHEN[1]

[1]*Department of Computer Science and Information Engineering*
Chaoyang University of Technology
Taichung, 413 Taiwan

[2]*Department of Mechatronics Engineering*
National Changhua University of Education
Changhua, 500 Taiwan

With the technology improving, many content-services have been digitalized constantly in our daily life. To be more convenient and efficient, many kinds of high technological products have also been personalized, mobilized, and people can handle their businesses at any time from anywhere. For example, mobile users can perform the Internet transactions via mobile devices (such as cell phone and Personal Digital Assistant). Nowadays, the cell phone is not only used in communication, but it can be combined with Personal Digital Assistant (PDA) functions. The progress of technology makes the commercial activities efficient; moreover, it also provides consumers with more convenient and intimate services. On the basis of the tendency, we implement a digital value-added services platform via PDA in this research. We integrate the related cryptography mechanisms (for example: public key, secret key cryptography system and digital signature) wireless and SQL technologies to construct a real-time and secure mobile ticket system. The consumer can use a mobile device to get a requested value-added service such that the buyers and sellers can perform a secure transaction. Therefore, the security and reliability of the system are assured in our scheme.

Keywords: RSA, security, mobile ticket, digital signature, mobile devices, verification

1. INTRODUCTION

1.1 Motivations

With the improvement of life, a large proportion of recreation and arts activities are held everywhere Cultural events, such as movies, concerts, opera, and sports, allow us to enjoy the performances by purchasing tickets. At early times, it was in the designated location that these kinds of tickets were purchased. Nowadays, even though people book or buy tickets on the Internet, they still have to take their tickets at the appointed ticket window. What's more, tickets could be lost or stolen. Sometimes paper tickets may be falsified or reproduced. When one temporarily wants to make a purchase of a ticket, he/she may stand in line to have the ticket purchased at the ticket window. This seems to be an inconvenient consuming behavior. Therefore, we hope a real-time and secure mobile ticket system operation platform can be well constructed to reduce the annoyances and inconveniences mentioned above.

Received February 1, 2008; accepted November 28, 2008.
Communicated by Yau-Hwang Kuo, Pau-Choo Chung and Jar-Ferr Yang.
* This work was partially supported by the National Science Council of Taiwan, R.O.C. under grant No. NSC 97-2221-E-324-013.

1.2 Purposes

There were plenty of shortcomings and inconveniences in the outdated ticket-purchase-system. For example, we could not get the tickets in time, and the procedures to purchase and collect the tickets are trivial and time-consuming.

Since many problems existing in the ticket-purchase-system, there is an urgent need to have a set of real-time mobile ticket system. Based on the digital value-added services platform via PDA, we integrate the technologies of wireless communication, cryptography and electronic commerce to provide a real time mobile ticket system, in which technology delicately blends with life to meet people's need.

1.3 The Applications of the Ticket System

The applications of the ticket system are widely used, and they are closely linked to our daily life. For example, we buy tickets to see a movie, enjoy the basketball or baseball games, book train tickets, or high speed train tickets, and any performances (dance, drama, concerts, *etc.*). The ways to purchase the tickets can be classified into three main types-Windows Ticketing, Voice Ticking, and Internet Ticking.

If we buy the tickets by the way of Windows Ticketing, Voice Ticking or Internet Ticket, basically the places to collect the tickets can be either the ticket-selling points of the administration (such as theaters, ticket offices at baseball or basketball games, train stations, airports) or chain of retail stores in the neighborhood (such as post offices, convenience stores).

Whatever methods consumers may take, they are required to go to the appointed places to collect their purchased tickets. This inconvenience has not been effectively solved for a long time. Since the ticketing system has a significant influence on human's life, how consumers can efficiently and conveniently purchase and collect their tickets is what we are examining. The aim of this research is to solve the inconveniences the consumers may encounter.

1.4 Review the Related Technologies and Researches

Once the ticket is purchased or collected, the security and reliability of the transaction for ticket information cannot be emphasized too much. Hence, the security of the information transmission will be taken into consideration. Based on this requirement, we intend to integrate the encryption/decryption methods with the database system to implement an "all-in-one" real time mobile ticket system. In this research, the RSA encryption/ decryption system and the related technologies will be discussed briefly later.

1.4.1 RSA cryptographic algorithm

RSA algorithm is an encryption/decryption technology for public-key cryptosystem which is widely used in electronic commerce [1]. The algorithm was publicly described in 1978 by Ron Rivest, Adi Shamir and Leonard Adleman at MIT and was granted US patent 4405829 [2]. The RSA algorithm is showed as follows:

Step 1: Choose two large random prime numbers p, q, and $p \neq q$; compute $n = p \times q$.
Step 2: Compute totient $\phi(n) = (p - 1)(q - 1)$, and $\phi(n)$ is the Euler's Function.
Step 3: Compute d to satisfy the congruence relation $e \times d = 1 \bmod \phi(n)$.
Step 4: Announce the (e, n) in public directory, and the other parameters are kept secret.

Encrypt messages are as follows:

(1) Suppose A sends a plaintext "M" to B.
(2) B transmits public key n and e.
(3) A uses the format that A and B negotiated initially. A then computes the cipher text C as follows: $C = M^e \bmod n$.

Decrypt messages are as follows:

(1) B can recover M from C by using his/her private key d to decrypt the received message in the following procedure: $C^d \bmod n = M^{ed} \bmod n = M$.
(2) The receiver B can recover the original message "M."

The security of the RSA algorithm which is based on the difficulty of the $n = p \times q$ factorization. Nowadays, the $n = p \times q$ is at least 1024 bits long for security. Even though we use the fastest computer to decompose the large prime n into two primes p and q product, it still takes a long time. Therefore, the RSA algorithm applied to the business applications remains secure. In our scheme, the Verification Server which communicates the related ticket information with the Ticket Server should be kept confidential; otherwise, once the information is leaked out, the security will be faced with challenges. Consequently, we apply the RSA encryption/decryption algorithm to construct a secure channel. Only when the mobile user and the mobile device pass the Verification Server's authentication can the mobile user enjoy the exhibition or the program.

1.4.2 Signature with one-way hash function

The one-way hash function has been used in computer science for a long time [3]. It requires a variable-length input string (called a pre-image) and converts it to a fixed-length input string (called a hash value). A one-way hash function works in one direction. It is easy to compute a hash value from a pre-image, but it is hard to generate a pre-image that hashes to a particular value. For example, a function h: $X \rightarrow Y$ is one way. If it is easy to compute $h(x)$ for every $h \in X$, yet it is hard for most $y \in Y$ to figure out an $x \in X$ such that $h(x) = y$. A more formal definition of one-way functions can be found in [4].

In practice, h is constructed to use a standard collision resistant hash function whose values are, for example, 160 bits strings. The signature of the document x is $S = h(x)^e \bmod n$. From this signature, only the hash value $h(x)$ but not the document x can be reconstructed. For instance, Bob can only verify the signature of x if he also knows the document x. After Alice computes the signature s of x, she sends s together with the document x to Bob. Bob computes $m = s^e \bmod n$ and compares this number with the hash value of x. Since the hash function is public, Bob can compute this hash value. If m is equal to x, Bob can definitely accept the signature. Otherwise, he rejects it [5].

1.4.3 Mobile ticket

With the popularity of mobile phones and the increasing transmitting speed, the application of mobile tickets has been developed in our daily life. A wider variety of tickets lead to a new trend, in which electronic tickets that are downloaded or stored from mobile phones and portable PDA devices gradually replace the traditional paper tickets. Electronic tickets not only save time that users might spend more in waiting in line in the past, but they don't have to carry all kinds of tickets with themselves. Mobile phones as well as portable PDA devices are just like an electronic wallet which can store electronic tickets, which are very convenient for users to manage and use [6-10].

1.4.4 Electronic commerce service

Mobile commerce brings the new niches and commerce profits for researchers and service providers [11]. However, the researchers [12-15] pointed out the application bottleneck for using mobile device.

Electronic commerce, commonly known as e-commerce, uses the Internet and the WWW to transact business. More formally, e-commerce is considered to be digitally enabled commercial transactions between and among organizations and individuals. Basically, the type of Electronic Commerce is divided into the following types:

(1) B2C: Business to Customer
(2) B2B: Business to Business
(3) C2C: Customer to Customer
(4) P2P: Peer to Peer
(5) M-commerce: Mobile commerce

Besides, the advantages of the Mobile Commerce consist of the following features, which are listed in Table 1. This shows that the developments of the Mobile Commerce and the human life are closely related. Compared with traditional business, the Mobile Commerce can overcome space-time limitations to create a lower cost and a flexible business environment. To provide a simple operation as well as a secure and convenient transaction in purchasing and collecting ticket system is the trend of the times. For this reason, we refer to the related literatures [16-19] to construct a real time and secure mobile ticket system.

Table 1. The advantages of mobile commerce.

Ubiquity	Internet/Web technology is available everywhere: at work, at home, and everywhere via mobile devices, anytime.
Global Reach	The technology reaches across nation boundaries, around the earth.
Universal Standards	There is one set of technology standards, namely Internet standards.
Richness	Video, audio, and text messages are possible.
Interactivity	The technology works through interaction with the user.
Information Density	The technology reduces information costs and raises quality.
Personalization/ Customization	The technology allows personalized messages to be delivered to individuals as well as groups.

Table 2. The disadvantages of mobile commerce.

Function	The small screen and small functional key area.
Limited	1. The limited computing power, memory and disk capability. 2. The limited battery life. 3. The limited browsing capability. 4. The limited graph format.
Standards	1. The complex characters input method. 2. The error probability of the data storage and transaction is higher. 3. The diversity of operation system.
Interactivity	Unfriendly user interface.
Cost	Expensive communication cost.

We list the disadvantages of Mobile Commerce in Table 2. This shows limitations and disadvantages which leave something to be desired.

1.4.5 Bluetooth technology

The Ericsson Mobile Platforms established a project in 1994 and wanted to have the limit of electric wire taken out such that the mobile phone could be connected to the wireless phone. Later, Bluetooth Special Interest Group, Bluetooth SIG, was composed of Ericsson, Nokia, Intel, IBM, and Toshiba to constitute the standard of short-range wireless connection, which was named Bluetooth [20].

Bluetooth Technology can support the wireless transmission of the computer, communication, and other kinds of devices. Bluetooth is a radio standard and communication protocol primarily designed for low power consumption with a short range and low cost. The charm of Bluetooth technology lies in its integrated open platform, which enables the related information devices with Bluetooth chips to connect such devices as mobile phones, notebooks, personal digital assistants (PDAs), PCs, and other peripheral products without electric wires. Moreover, since the manufacturers do not have to pay patent fee and royalty payment, lots of manufacturers get down to investing in this new market.

The main characteristics of Bluetooth Technology involve wireless transmission, higher security, piconet, and interoperability [21].

1.4.5.1 Wireless transmission

Bluetooth replaces electric wire to adopt wireless communication and is connected to the device of the Bluetooth chip. The range of transmission is within 10 meters, and the speed of transmission is 1 MB/second. If the Frequency Amplifier is added, the range of transmission can be as far as 100 meters.

1.4.5.2 Higher security

Bluetooth can set up the encryption for protection, and use frequency hopping spread spectrum (FHSS) (1600/minute); it is hard to be intercepted and to be interfered by electromagnetic radiation. Therefore, Bluetooth can guarantee higher security.

1.4.5.3 Piconet

Bluetooth can be one to one or one to more, each of which connects each other to form a network of Bluetooth. This network group can support up to eight devices, one of which is called "master," while the others are called "client." Because each piconet can be a member of other Bluetooth networks, the links and links of the networks will form the Ad-hoc computer network. Bluetooth can support the synchronous and the asynchronous transmission mode. Therefore, it is easy to integrate the Bluetooth networks with the TCP/IP networks.

1.4.5.4 Interoperability

Bluetooth does not need to use the face-to-face transmission like the communication port. Bluetooth is different from the IrDA transmission port which uses line-of-sight transmission. Besides, the Bluetooth transmission requires less power consumption than the IrDA transmission. This technology can be applied to set up a connection of good interoperability, low cost, and low power.

Nowadays most portable PDA devices have been equipped with the Bluetooth transmission function. This mobile ticket system takes advantage of the characteristics of being low-power, economizing electricity, speedy transmission, and long-distance transmission in Bluetooth. After purchasing and collecting the ticket, the consumer carries the portable PDA device to the verification server. We adopt the Bluetooth transmission function to transmit the mobile ticket which is stored in the PDA for the verification server to decrypt and verify. Simultaneously, the double spending will be detected.

2. SYSTEM STRUCTURE AND RESEARCH METHOD

2.1 Outline of the System Structure

Fig. 1 stands for the system structure in this study, and the functions of the roles are defined as follows:

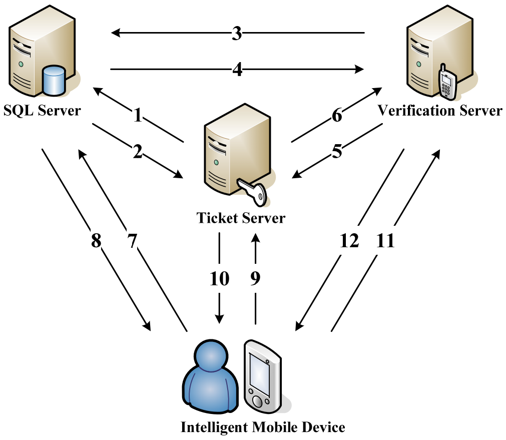


Fig. 1. System structure.

(1) Intelligent Mobile Device: The client's mobile device can query information and buy the ticket.
(2) SQL Server: Preserve various data.
(3) Ticket Server: Information processing, generation of the mobile ticket, creation of the key to encrypt/decrypt.
(4) Verification Server: Verify the client's mobile ticket.

The protocol is composed of four phases, namely, key generation phase, servers' communication phase, shopping phase, and authentication phase. One party that wants to communicate with another party should send a request message *M* and make a signature *S* (such as RSA digital signature) to make a request. Only the signature is authenticated, the proposed request will be accepted and similarly will return a response message with a signature. Thus, we suppose at least a message (*S*, *M*) should be sent to the opposite party when they would like to communicate with each other.

The functions inside and the procedures are described as follows:

(1) Key generation phase:
Step 1: According to the request, the Ticket Server searches for information from the SQL Server, and generates the key pairs for encryption/decryption.
Step 2: The SQL Server returns the request information for the Ticket Server.

(2) Servers' communication phase:
Step 3: The Verification Server according to its demand to search for ticket information from the SQL Server, and gets the decryption key from the Ticket Server.
Step 4: The SQL Server returns the response information for the Verification Server.
Step 5: The Verification Server proposes a decryption key request to the Ticket Server.
Step 6: The Ticket Server returns the decryption key to Verification Server.

(3) Shopping phase:
Step 7: The Client searches for various kinds of ticket information from the SQL Server.
Step 8: The SQL Server returns the ticket information to the Intelligent Mobile Device needs.
Step 9: The client makes a request for the purchase of the ticket from the Ticket Server, and the mobile ticket will be created from the Ticket Server.
Step 10: The Ticket Server returns the mobile ticket to the client.

(4) Authentication phase:
Step 11: The client is connected to the Verification Server via the mobile device to verify the mobile ticket.
Step 12: The Verification Server shows the result of the verification and returns it to the client.

2.2 Research Methods

According to the mentioned requirements, we can divide the main system into four sub-functions: PDA Mobile Device, SQL Server, Ticket Server and Verification Server. Fig. 2 is the organization chart of this system.

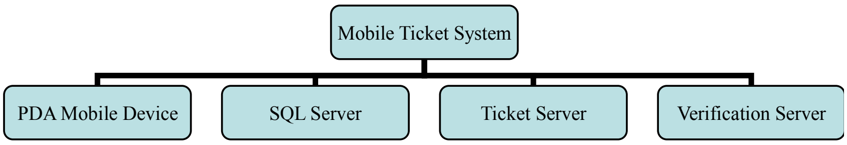


Fig. 2. System organization chart.

2.2.1 PDA mobile device

The customers can login, browse, and retrieve the related information of the tickets they want, such as the name of the activity, time, place, ticket price, *etc.* The content is introduced by pictures and articles, which helps the users to understand the related information while they are querying the content of service.

Figs. 3-5 is the PDA forms for the customer to use the mobile ticket system. Fig. 3 is the login form, in which the customer must enter the user's account and password to login; Fig. 4 is the main form of this system, in which the customer can either choose the functions in the system or choose whatever tickets he wants. Fig. 5 is the browser form of the ticket information, in which the customer can query the content of activities and introduction.

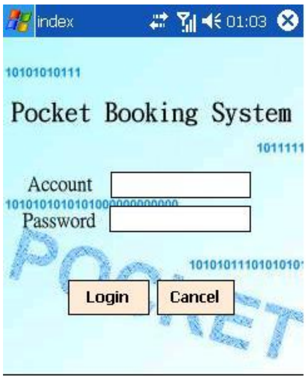
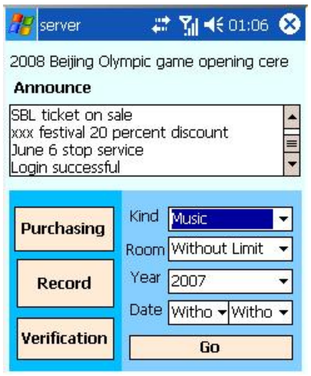


Fig. 3. PDA mobile device system: login form.



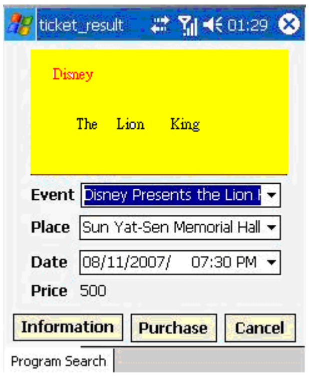
2008 Beijing Olympic game opening cere

Announce

SBL ticket on sale
xxx festival 20 percent discount
June 6 stop service
Login successful

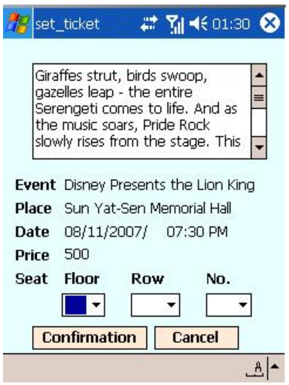
Kind Music
Room Without Limit
Year 2007
Date Witho Witho

Fig. 4. PDA mobile device system: main form.



Event Disney Presents the Lion K
Place Sun Yat-Sen Memorial Hall
Date 08/11/2007/ 07:30 PM
Price 500

Fig. 5. PDA mobile device system: browser form.



Giraffes strut, birds swoop, gazelles leap - the entire Serengeti comes to life. And as the music soars, Pride Rock slowly rises from the stage. This

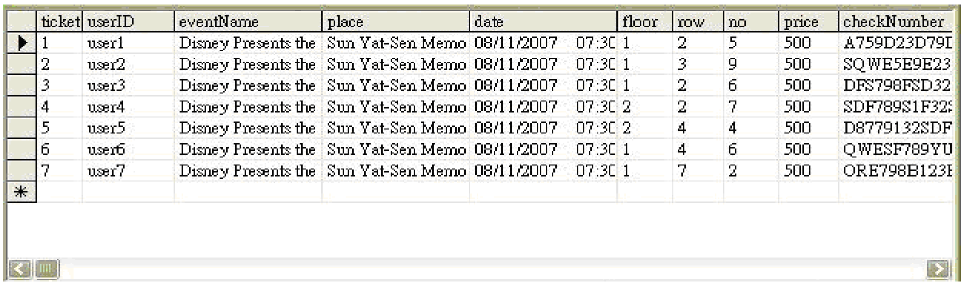
Event Disney Presents the Lion King
Place Sun Yat-Sen Memorial Hall
Date 08/11/2007/ 07:30 PM
Price 500
Seat Floor Row No.

Fig. 6. PDA mobile device system: purchase form.

When the customer finishes browsing and decides to buy the ticket for the specific number of showings, our system offers the function for the customer to book the ticket. After deducting the pre-paid point from the user, the system will immediately transmit a mobile ticket to the user's PDA. Before the mobile ticket is transmitted, it will be encrypted by RSA to prevent the third party from being falsified or reproduced. Fig. 6 is the form to purchase the ticket.

2.2.2 SQL server

It can store and record various related data of the store, customer's personal information, the quantity of the tickets that are sold. It is showed in Fig. 7.



	ticket	userID	eventName	place	date	floor	row	no	price	checkNumber
▶	1	user1	Disney Presents the	Sun Yat-Sen Memo	08/11/2007 07:3C	1	2	5	500	A759D23D79I
	2	user2	Disney Presents the	Sun Yat-Sen Memo	08/11/2007 07:3C	1	3	9	500	SQWE5E9E23
	3	user3	Disney Presents the	Sun Yat-Sen Memo	08/11/2007 07:3C	1	2	6	500	DFS798FSD32
	4	user4	Disney Presents the	Sun Yat-Sen Memo	08/11/2007 07:3C	2	2	7	500	SDF789S1F32
	5	user5	Disney Presents the	Sun Yat-Sen Memo	08/11/2007 07:3C	2	4	4	500	D8779132SDF
	6	user6	Disney Presents the	Sun Yat-Sen Memo	08/11/2007 07:3C	1	4	6	500	QWESF789YU
	7	user7	Disney Presents the	Sun Yat-Sen Memo	08/11/2007 07:3C	1	7	2	500	ORE798B123I
✱										

Fig. 7. SQL server data record.

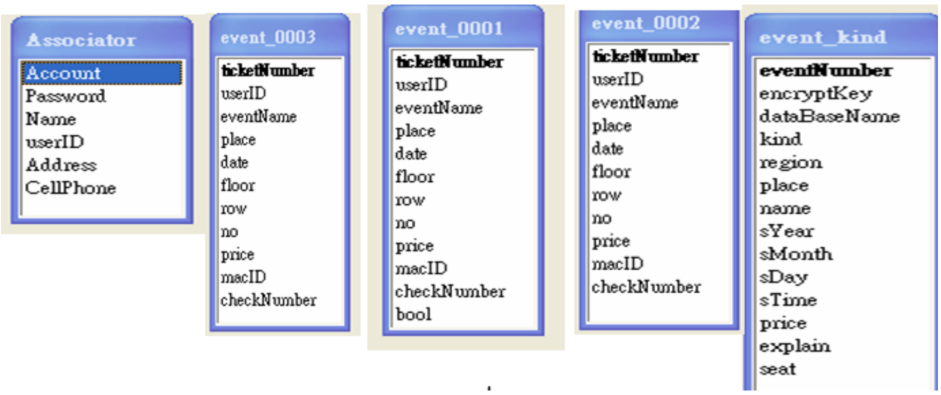


Fig. 8. SQL server data schema.

The SQL Server Data Schema are showed in Fig. 8. The SQL Server Data Schema include six items, as follow: (1) event_kind (records the related information of every show); (2) Event_00001 (the last four number is the number of the showings which records the ticket-purchase situation); (3) place_all-kind (information of the place); (4) Associator (member's data); (5) show_message (announcement); (6) other (open year).

Fig. 9 is the SQL server E-R diagram, which describes the relations among the six tables. The SQL Server E-R Diagram is showed in Fig. 9.

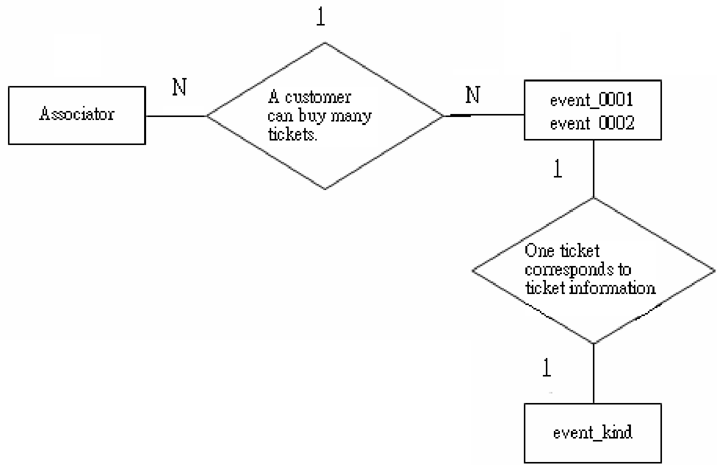
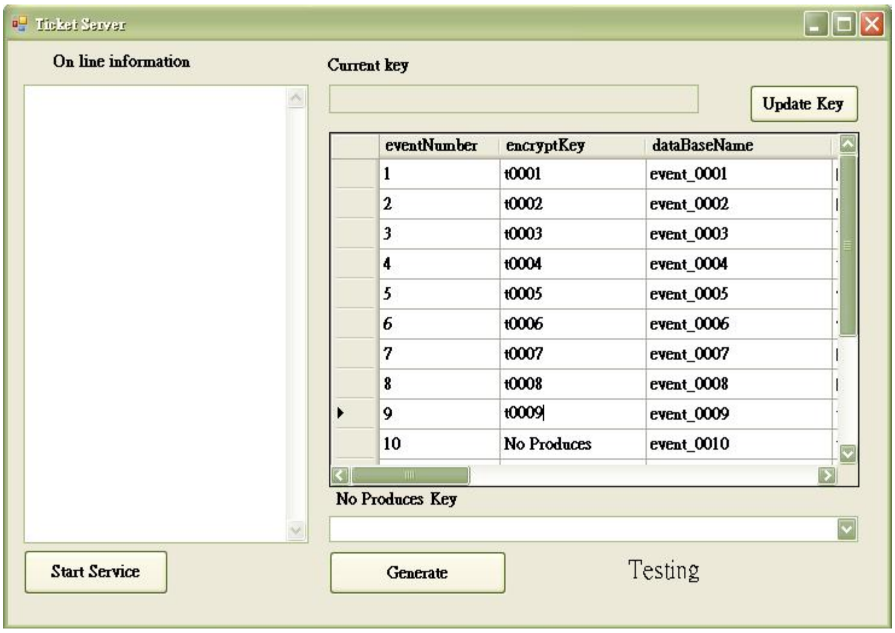

1
N
Associator
A customer can buy many tickets.
N
event_0001
event_0002
1
One ticket corresponds to ticket information
1
event_kind

Fig. 9. SQL server E-R diagram.



eventNumber	encryptKey	dataBaseName
1	t0001	event_0001
2	t0002	event_0002
3	t0003	event_0003
4	t0004	event_0004
5	t0005	event_0005
6	t0006	event_0006
7	t0007	event_0007
8	t0008	event_0008
9	t0009	event_0009
10	No Produces	event_0010

Fig. 10. The ticket server generates ticket form.

2.2.3 Ticket server

The ticket server is responsible for the whole information processing in the system. After the customer purchases the ticket, the key pairs will be generated for encryption/decryption, and the mobile ticket will be generated by the ticket server as well. The ticket form is showed in Fig. 10.

2.2.4 Verification system

When the customer arrives at the site of the activity, the verification system will collect and verify customer's ticket. The mobile ticket in the customer's PDA will be transmitted to the verification server by Bluetooth. The verification server will decrypt and check up whether the mobile ticket is the correct one for this show or not, and it can also identify if the double spending occurs. Fig. 11 is the verification system.

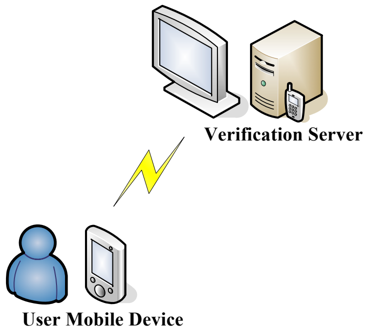


Fig. 11. Verification system.

2.3 Hardware and Software Specifications

Software

(1) Microsoft Visual Studio.net 2003 [22].
(2) Microsoft SQL Server 2000 Developer Edition-Database Server [23].
(3) PDA Client software.
(4) PC Server software.
(5) ActiveSync 4.2.

Hardware:

(1) PDA: HP iPAQ hx4700.
(2) Bluetooth Transistor.
(3) PC Server: AMD Athlon 1.81GHz, 512MB.
(4) Verification Server.

2.4 System Evaluations

This paper mainly constructs a real time and secure mobile ticket system. Before the system is integrated, we have to reassure all designed components can output correctly. We have the unit test and integration test, stress test, regression test and acceptance test. According to the system requirement specification and the system design document, the project and the content related to the integration test will be described in this paper. By describing and realizing this testing project, we hope the testing tasks can go well.

(1) A variety of tests will be held in the period of the implement and integration test. If

we want to add a new module to the previous formula which has been tested, then it is necessary to have a unit test, and integrate an integration test.

(2) Stress test is a testing work in which the software products will be normally done. The process is to ensure that the software products can be executed without errors when the load work of the software products reaches a high point. In our system, when a number of people login to make online purchases of the mobile tickets simultaneously, the system can still be operated well.

(3) Regression test is the period when any bug is found in testing formula. After being modified, the formula has to be tested again to ensure it can run well.

(4) Acceptance test has to meet the following requirements:
The necessary requirements, including critical needs, important needs and desirable needs, have to undertake a complete test. The testing procedures will proceed as planned. All testing results have to accord with the expecting testing result. Once the testing fails, the unit test is required and the testing principles are the same as the former.

This system integrates related technologies – wireless network communication, cryptography, and database to reach a considerable integration and reliable security.

3. RESULTS AND DISCUSSION

This research integrates the cryptography and the technology of mobile communication successfully to construct a more open, fair, secure and much more mature mobile commerce environment. The requirements and the functions that are attainable will be discussed as follows:

3.1 Experimenting Platform

The overall objective of this research is that the electronic commerce can be introduced by the concept of the mobile ticket. The experimenting platform of the real-time mobile ticket system can be well constructed and projected by the characteristics of the mobile ticket, which is based on the complete database, and it can also bring about some advantages:

(1) Simplify the procedure of purchasing the ticket.

(2) The customers do not need to spend extra time collecting their tickets at the specific ticket window.

(3) Reduce the cost for management and the human resources.

The structure of the electronic commerce website is illustrated as follows:

(1) Product overview pages:
It provides the consumers with the products they want. The search engine that is inclusive of the merchandise makes the consumers find what they want faster and more easily.

(2) The discussion board of products:
After using the product, the consumers may feel free to make a comment on it for other consumers to know how they feel about the product or notify the administrator of any revisions in this system.

(3) The real times news system:
The consumers may take hold of the renewed data or other related service information after they get onto the homepage.

(4) The products updated and the shelf uploaded:
The server can register the new products in a simple way and provide the illustrated introduction for the consumers to search.

(5) Login and security design:
When the consumer makes a purchase, it can guarantee the personal information is not disclosed and effectively store every consumer's related history information in the system.

(6) Shopping cart:
The consumer can easily examine what he wants to purchase and choose the payment method.

Through this experimenting platform, the corresponding relations exist in the mobile tickets, electronic commerce, the databases and the integrated mode, which will be formed to provide the mobile ticket system an instant, convenient, efficient and accurate integration. It can also promote the security of the mobile ticket to keep up with the trend in the future.

3.2 Security Issue

This system is combined with the RSA encryption/decryption algorithm. We use the encryption/decryption algorithm to transmit data over the Internet. Based on the difficulty of the decomposing the factor, as long as the user assures that he/she will not disclose the private key, the security of the data can be well guaranteed.

3.3 Convenience Issue

This system makes use of the portability of the PDA device very well. As long as the users are surrounded by the signals of wireless communication, they can browse and search the information for the ticket service. This can completely avoid the previous awkward situation – the consumer must collect the ticket in person or even spend more time waiting in line.

3.4 Just-in-time Issue

The transmission between our mobile ticket system and the wireless network communication enables the consumers to purchase and collect their tickets simultaneously without spending extra time completing the purchase procedure. There are no limits for space-time to purchase and collect tickets.

3.5 Database Issue

This system makes use of SQL Server Database to manage the storage of information. Here are several advantages:

(1) With higher capacity and efficiency, it promotes the speed of access to database.
(2) It is easy to use and manage. Even the non-programmers and non-professionals can operate SQL easily.
(3) The application of database strengthens the convenience. The other platforms can use SQL to query, and modify in the database.

3.6 No Forging Issue

No one can generate the valid mobile ticket signature except the Ticket Server. It is actually infeasible for anyone to forge the signature without knowing the Ticket Server's private key.

3.7 Efficient Ticket Verification Issue

In our scheme, the key pairs are generated by Ticket Server via off-line model. The Verifier Server can independently verify the mobile ticket and MAC (Message Authentication Code) of the mobile device. Once the mobile ticket is used, the database will delete the related information, and the double spending will be detected easily.

We arrange a stress test in which one thousand users or the mobile device will simultaneously login to our system to see how the system may work when carrying a heavy load. They are respectively asked to enter their ID for 30 times and make an online purchase for 70 times. The total data for testing have 10,000 records. Stress test is a testing work in which the software products will be normally done. The process is to ensure that the software products can be executed without errors when the load work of the software products reaches a high point. In our system, when a number of people login to make online purchases of the mobile tickets simultaneously, the system can still be operated well.

3.8 Practicability Issue

We proposed complete scenarios that include the ticket request, issue and verification phase for a mobile ticket infrastructure. Our scheme meets important issues about the ticket system. It is easily applied to the current mobile system and network without any needs of extra infrastructures.

3.9 Delay and Bandwidth Issue

According to J. Kurose, and K. Ross [24], there are four sources of the packet delay existing in the network transmission, as shown in Fig. 12. However, these are not invariable. It depends much on various factors, instead.

For example, we use the Fig. 13 to illustrate the queuing delay condition as follows:

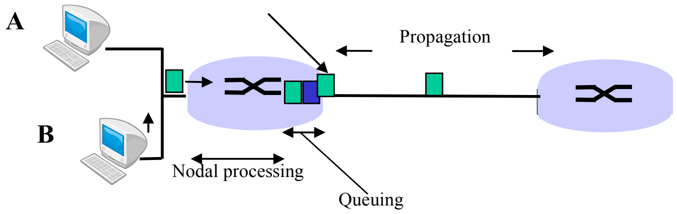


Fig. 12. Four sources of packet delay.

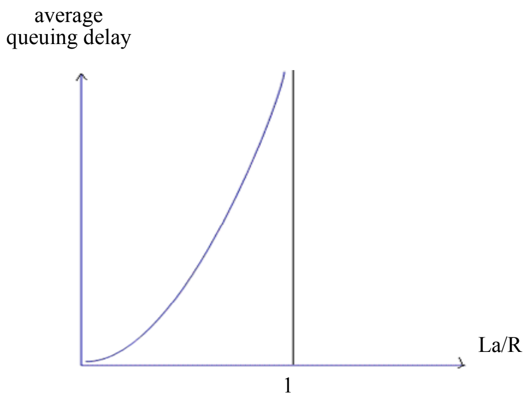


Fig. 13. Queuing delay.

If the nodal delay is d_{nodal}, then $d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$

where d_{proc} = processing delay typically a few microseconds or less
d_{queue} = queuing delay depends on congestion
d_{trans} = transmission delay = L/R, significant for low-speed links
d_{prop} = propagation delay, a few microseconds to hundreds of micro seconds

The related descriptions about queuing delay are described as follows:

R = link bandwidth (bps)
L = packet length (bits)
a = average packet arrival rate
La/R ~ 0: average queuing delay small
La/R -> 1: delays become large
La/R > 1: more “work” arriving than can be serviced, average delay infinite.

In order to emphasize the fact that the proposed scheme is effective in transmitting messages, we present the transmission time in the Internet environments (in 1 Mbps and 56 Kbps) for each phase in Table 3.

In Table 3, we find the fixed transmission time is short. The proposed system is practical. Take the server for example. When each data is transmitted, the speed of 20

Table 3. The communications of the transmission data.

Phase	Rounds of communication	Communication amounts (bits)	Data transmission time (ms)	
			1 Mbps	56 Kbps
Key generation phase	2	$2\|M\| + 2\|S\| + n\|K\|$	$2.064 + (n\|K\|/1000)$	$36.857 + (n\|K\|/56)$
Servers' communication phase	4	$4\|M\| + 4\|S\|$	4.128	73.714
Shopping phase	4	$4\|M\| + 4\|S\|$	4.128	73.714
Authentication phase	2	$2\|M\| + 2\|S\|$	2.064	36.857
Total	12	$12\|M\| + 12\|S\| + n\|K\|$	$12.384 + (n\|K\|/1000)$	$221.142 + (n\|K\|/56)$

Notes: Suppose $|M|$ is the length of message (1 byte); $|S|$ is the length of a RSA digital signature (1024 bits); $|K|$ is the length of RSA encryption/decryption key (1024 bits); n is the amount of the issuing key for Ticket Server.

Kbps is required. If the bandwidth from ADSL is 2GB per month, then 100,000 bps per month. That is, about 3500 records are for each day. If the average booking of each guest is 5, then the server can accept about 700 guests to book the ticket each day.

4. CONCLUSIONS

We propose the integration of the technical applications for the portable PDA device, the Bluetooth transmission, the mobile ticket, electronic commerce, SQL databases, and implement a secure mobile ticket system. By the capability of the management in SQL, the convenience and popularity of the PDA device, a swift search of the web pages, and the convenience of the Bluetooth transmission, our system manifests the real time characteristic, features the convenience of the ticket purchasing system, and effectively saves consumer's time to collect tickets and reduces inconveniences. With the consuming information that is collected from the system, a lot of users' expenditure behavior and habits can be analyzed as the reference resources for the manufacturers to offer much more popular activities, and to attract more consumers in order to be assured of an utmost beneficial result.

REFERENCES

1. S. L. Garfinkel, "Public key cryptography," *Computer*, Vol. 29, 1996, pp. 101-104.
2. R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, Vol. 21, 1978, pp. 120-126.
3. Y. Y. Chen, J. K. Jan, and C. L. Chen, "A fair and secure mobile billing system," *Computer Networks*, Vol. 48, 2005, pp. 517-524.
4. S. Goldwasser, "The search for provably secure cryptosystems," in *Proceedings of Symposium in Applied Mathematics*, Vol. 42, 1990, pp. 89-113.
5. J. A. Buchmann, *Introduction to Cryptography*, 2nd ed., Springer-Verlag, New York, 2004.

6. Y. Y. Chen, J. K. Jan, and C. L. Chen, "Design of a fair proxy raffle protocol on the internet," *Computer Standards and Interfaces*, Vol. 27, 2005, pp. 417-424.
7. A. Mana, J. Martinez, S. Matamoros, and J. M. Troya, "GSM-ticket: Generic secure mobile ticket service," in *Proceedings of GEMPLUS Developer Conference*, 2001, pp. 1-7.
8. B. Patel and J. Crowcroft, "Ticket based service access for the mobile user," in *Proceedings of the 3rd Annual ACM/IEEE International Conference on Mobile Computing and Networking*, 1997, pp. 223-233.
9. H. Wang, J. Cao, and Y. Zhang, "Ticket-based service scheme for mobile users," in *Proceedings of the 25th Australian Computer Science Conference on Research and Practice in Information Technology*, 2002, pp. 285-292.
10. Y. Y. Chen, C. L. Chen, and J. K. Jan, "A mobile ticket system based on personal trusted device," *Wireless Personal Communications*, Vol. 40, 2007, pp. 569-578.
11. K. C. Lauden and C. G. Traver, *E-Commerce*, *Business*, *Technology*, *Society*, 2nd ed., Addison Wesley, New York, 2002.
12. S. S. Grosche and H. Knospe, "Secure mobile commerce," *Electronics and Communication Engineering Journal*, Vol. 14, 2002, pp. 228-238.
13. A. Tsalgatidou, J. Veijalainen, and E. Pitoura, "Challenge in mobile electronic commerce," in *Proceedings of the 3rd International Conference on Innovation through E-Commerce*, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.31.7254&rep=rep1&type=pdf, 2000.
14. A. Tsalgatidou and E. Pitoura, "Business models and transactions in mobile electronic commerce: Requirements and properties," *Computer Networks*, Vol. 37, 2001 pp. 221-236.
15. J. Veijalainen, V. Terziyan, and H. Tirri, "Transaction management for m-commerce at a mobile terminal," in *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*, 2003, pp. 10.
16. P. C. Ho, "Design and implementation of a fair and secure mobile commerce system," Master Thesis, Department of Computer Science, National Chung Hsing University, Taiwan, 2004.
17. H. B. Chen, "A study of mobile ticketing," Master Thesis, Department of Information Management, Chaoyang University of Technology, Taiwan, 2003.
18. Information and Communication Security Technology Service Center (ICST) Forum, http://forum.icst.org.tw/phpBB2/.
19. Commerce Net Taiwan website, http://www.commercenet.org.tw/.
20. C. L. Hsu, "Bluetooth technology," Academia Sinica Computing Centre, Vol. 18, 2002.
21. Bluetooth, Special Interest Group, SIG, http://www.bluetooth.com/bluetooth/.
22. Microsoft MSDN website, http://www.microsoft.com/taiwan/msdn/default.mspx.
23. Microsoft SQL Server, http://www.microsoft.com/taiwan/sql/.
24. J. Kurose and K. Ross, *Computer Networking: A Top Down Approach Featuring the Internet*, 3rd ed., Addison-Wesley, 2004.

Chin-Ling Chen (陳金鈴) was born in Taiwan in 1961. He received the B.S. degree in Computer Science and Engineering from the Feng Chia University in 1991; the M.S. degree and Ph.D. in Applied Mathematics at National Chung Hsing University, Taichung, Taiwan, in 1999 and 2005 respectively. He is a member of the Chinese Association for Information Security. From 1979 to 2005, he was a senior engineer at the Chunghwa Telecom Co., Ltd. He is currently an assistant professor of the Department of Computer Science and Information Engineering at Chaoyang University of Technology, Taiwan. His research interests include cryptography, network security and electronic commerce.

Yeong-Lin Lai (賴永齡) received the Ph.D. degree from the Institute of Electronics, National Chiao Tung University, Taiwan, R.O.C., in 1997. From 1985 to 1989, he was with the Electronic Systems Research Division, Chung-Shan Institute of Science and Technology, Taiwan, where he worked in the field of electronic system design and testing. From 1992 to 1993, he was a Senior Engineer at Macronix, Inc., Hsinchu, Taiwan, where he was engaged in VLSI design. From 1993 to 1997, he joined the research programs at Hexawave, Inc., Taiwan, where he was engaged in the development of microwave semiconductor devices and circuits. From 1997 to 1998, he was with the Department of Electronic Engineering, Minghsin University of Science and Technology, Taiwan, as an Assistant Professor. From 1998 to 2001, he was an Assistant Professor of the Department of Electronic Engineering, Feng Chia University, Taiwan. Since 2001, he has been with National Changhua University of Education, Taiwan. In 2001 and 2003, he was the visiting scholar of Communication Research Center, Ottawa, Canada. Dr. Lai is currently with the Department of Mechatronics Engineering and the Graduate Institute of Display Technology, National Changhua University of Education, as an Associate Professor. He is also an Adjunct Associate Professor of the Graduate Institute of Communication Engineering and the Graduate Institute of Integrated Circuit Design, National Changhua University of Education. His research interests include mobile communication, RFID, RFIC, NEMS, and display technologies. Dr. Lai received the Excellent Ph.D. Dissertation Award for Industries from Ministry of Education, Taiwan, R.O.C., in 1997. From 2004 to 2006, he received the Creation and Invention Award of National Changhua University of Education annually. In 2006, he received the Superior Mentor Award and the Superior Professor Award of National Changhua University of Education. In 2007, he received the Academic Research Award and the Outstanding Teaching Award of National Changhua University of Education.

Chih-Cheng Chen (陳志成) is a Lecturer in Department of Industrial Engineering and Management in National Chin-Yi Institute of Technology. He teaches IE & M courses in Automatic Data Capture System. From 1996 to 2004, he was a senior engineer of Syntegra Tech. Company, which is an integration application software provider for the enterprise. He earned a Master Degree in Department of Mechatronics Engineering from National Changhua University of Education in 2005. Now, he is a Ph.D. candidate in Department of Mechatronics Engineering from National Changhua University of Education in Taiwan. He has been practicing the RFID application system in many fields such as the patrol system and the long-term care of elders. His research interests include mobile technology and RFID applications.

Kun-Chih Chen (陳坤志) was born in Taiwan in 1985. He received the B.S. degree in Department of Information Engineering and Computer Science from Chaoyang University of Technology, Taichung, Taiwan in 2007. His research interests include cryptography, wireless networks and mobile commerce