Proceedings of the International Conference on Information Technology and Multimedia at UNITEN (ICIMU 2001)
Recent Advances and Future Trends in Information Technology and Multimedia
13th – 15th August 2001, Malaysia

`ATM IN YOUR POCKET'
A PROPOSED FRAMEWORK FOR A MOBILE E-ATM AND E-PAY

Ahmad Hisham Zainal Abidin
hishamza@uum.edu.my

Mohd Fairuz Shiratuddin
fairuz@uum.edu.my

University Utara Malaysia
06010 Sintok
Kedah Darulaman
Malaysia

ABSTRACT

Supposedly you need to do some online transaction at your Internet Banking website but you are not at your house or the office where your personal computer is. Hence, the use of a PDA with the ability to browse the Internet can perhaps overcome this problem. The question is how far local banks in Malaysia look at this small, compact and readily available device to access their Internet Banking websites. The purpose of this study is to identify the characteristics of Internet payment system at 3 local banks in Malaysia, whether the Internet Banking web site of each the banks supports the use of PDA and discusses how the bank's webmaster can make their website content relevant to PDA's users.

Keywords

Internet Banking System, Personal Digital Assistant, PDA

INTRODUCTION

Electronic Commerce (EC) has unleashed yet another revolution that is changing the way businesses buy and sell products and services. At present, EC is associated with buying and selling of information, products and services over the computer communication networks. EC technologies are designed to replace traditional paper-based workflow that is faster, more efficient with reliable communications between computers.

According to a study by International Data Corporation, e-commerce in Malaysia is poised to grow to more than RM35.72 billion by 2005 **[1]**. Therefore, Malaysian businesses are encouraged to take advantage of e-commerce and integrate it into their respective businesses.

With EC and the rapid growth in IT are undoubtedly changes the way we perform our daily activities. Buzzwords such as the e's and K's is regularly heard and talked about. In the same time our banking sector is slowly moving towards providing electronics transaction across the Internet. Banking transactions such as checking account balance, electronic cash withdrawal and transference using the Auto-Teller Machine or ATM and personal computer (PC), and also making payments for purchases are samples of activities that can potentially be mobile and wirelessly implemented. This can give the client a value-added advantage of performing the required transactions not only from home or the office, but also anywhere else within the location service coverage. Furthermore vehicle related issues such as parking, toll, petrol consumption no longer exists and one does not to be stuck in long queues.

Currently the use of mobile devices such as hand phones, pagers and Personal Digital Assistants (PDA) are getting popular amongst us. Although many of us use the PC as a mean to access the Internet, but many researchers believe that a paradigm shift will soon to happen i.e. the use of mobile devices to communicate and transact through the Internet.

In response to the above, EC's applications have to be designed in such a way the system will support access from various electronics device platforms ranging from the traditional PCs to PDAs and hand phones. A PDA was known to be just a device to store information e.g., addresses, appointments, memos, telephone numbers and schedules. Only until recently PDAs have used to

communicate effectively; e-mail and Internet access, and online transactions are now possible.

An interesting question arises! Since PDAs are being carried along in our pockets, why not use them to make electronics transactions **[2]**. Researchers are skeptical and attracted to study the how far is the capabilities of PDAs as devices that can electronically transacts the amount of money. The justification of PDAs being a device to engage with online transaction strongly lies within the concept of it being mobile, in comparison to the bulky and statuette nature of PCs. With the advent of PDA with Internet access, users can take the Internet with them, wherever they go. If the web site has information of use to a mobile professional, webmasters should consider optimizing their web site for viewing on a PDA **[3]**.

In 1999, local financial institutions in Malaysia have started to provide online banking and billing services. There are currently three online banks already offer Internet Banking services – Southern Bank Berhad, Hong Leong Bank Berhad and Malayan Banking Berhad (Maybank) with more expected to be launched in the next few months. The local online banking scene will get more competitive at the end of year 2001 when foreign banks are finally given the green light to offer online banking services in Malaysia.

The various online banking services share many common features including balance checking, transfer of funds between accounts and transaction summaries. Depending on the provider, some online accounts also support bills payment, stock trading, cheque-book requests, stop cheque payment request, online loan applications, financial planning tools and link to online merchants.

This paper try to give better understanding on how the ways the payment systems work by analyze the characteristic on Internet Payment System based on a scheme proposed by Lucas de Carvalho Ferreira **[4]** at Campus da UFLA, Brasil. The scheme consists of four subparts (Figure 1), each serving a single purpose:

i) describe payment systems typification through common characteristics
ii) present desirable requisites of payment systems
iii) describe system functioning from the user's perspective
iv) present implementation aspects of the system

Besides identifying the characteristics of Internet Payment System for each bank, second objective of this paper is to identify whether the Internet Banking web site of each bank supports the use of PDA, specifically PocketPC. Third objective is to discuss how bank's webmaster can make their website content relevant to PocketPC's user. Finally, the paper is concluded with summary and a discussion of the limitations of the study and future plan.

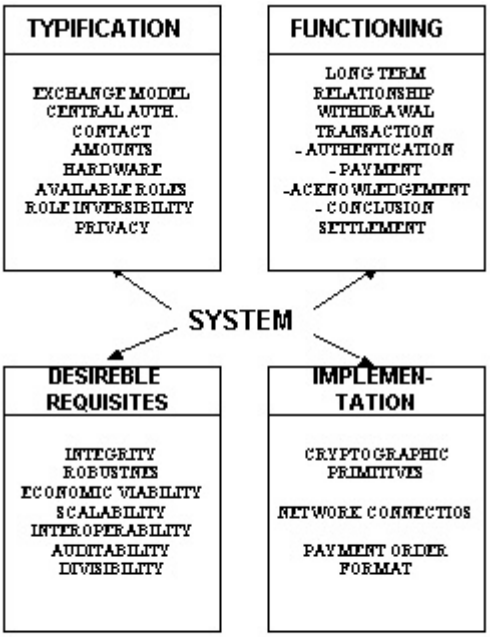

Figure 1 : Four Aspects that Characterize Electronic Payment Systems

THREE SYSTEMS IN DETAIL

1. Maybank2U.com

Maybank's online banking service can be access through www.maybank2u.com.my. The facilities offered by Maybank Internet Banking are familiar to what was offered through the Maybank Kawanku Phone Banking service. Customer can check account balance, transfer funds between customer's own account, transfer funds to 3rd party account within bank, future fund transfer, cancellation of future fund transfer and bill payment.

System Typification

Exchange Model: *Notational*. Payment is done by the settlement of balances in accounts managed by the bank. All clients' accounts in the most involved institution (Payee Corporation) including Syarikat Telekom Malaysia and Tenaga Nasional will be updated before next working day.

Central Authority Contact: *On-line*. The bank must be contacted during each transaction in order to verify all value transfers.

Payment Value: *Medium Payment*. System support only for value under RM3000.

Hardware: *General Purpose*. Only common computers are needed.

Possible Roles: Bank, Customer, Payee Corporation

Role Inversibility: *Unchangeable Role*. Each user has a predefine role.

Privacy: *Existent*. Privacy Protection Control systems are used to ensure that all transactions are secure, safe and confidential.

a) Username and Password – To prevent unauthorized access to Online Financial Services, every customer is required to select a username and password. This username and password is the access key to customer's financial information.
b) Data Confidentiality and Data Integrity – To ensure data confidentiality and data integrity, all information transmitted over the Internet is encrypted using the 128-bit Secure Socket Layer (SSL) from Verisign Certificate Authority. Strong end-to-end encryption is also adopted within the Bank's computer networks and resources including data center.
c) System Security and Monitoring – Firewall systems, strong data encryption, anti-virus protection and round the clock security surveillance systems to detect and prevent any form of illegitimate activities on bank's network systems.

Divisibility: *No divisibility* because the payment system is notational systems.

Desirable Requisites

Integrity: *guaranteed*. System Security and Monitoring.

Robustness: *None*

Economic Viability: *viable*

Scalability: *high*. The system is able to cope with the addition of new users and with the increase of the quantity of money involved in its operation without a significant loss of performance.

Interoperability: *no interoperability*. The system's design does not account for interoperability with other system.

Auditability: *guaranteed*. The system provides auditing facilities so that errors or misuse may be detected.

System Functionality Description

Establishment of Long Term Relationship: For new customer, they can log on to http://www.maybank2u.com.my and can apply their new account online. After three working days, customer can visit the branch they have selected to make an initial deposit, sign the specimen signature card and collect their ATM Card and PIN.

For existing customer and new customer that already have their ATM card, they can activate their Online Financial Services by going to any Maybank or Mayban Finance ATM machine. After they get their own 6 digits Maybank2u.com PIN, they have to log on to Internet to activate their online financial services.

Withdrawal: *none*

Transaction:

1. Request
2. Authorization
3. Customer Confirmation
4. Transaction Completion

Settlement: Bank deposit payee account and sent detail to payee.

Implementation Aspects

Cryptography: *N/A*

Network Connection: *N/A*

Payment order format: Each payment order includes the payment value, the access number (conversion from username) and password.

2. Southern Bank – SBB Direct Internet Banking System

Southern Bank's online banking service can be access through www.sbbdirect.com.my.

System Typification

Exchange Model: *Notational*. Payment is done by the settlement of balances in accounts managed by the bank.

Central Authority Contact: *On-line*. The bank must be contacted during each transaction in order to verify all value transfers.

Payment Value: *Medium Payment*. System support only for value under RM3000.

Hardware: *General Purpose*. Only common computers are needed.

Possible Roles: Bank, Customer, Merchant/Vendor

Role Inversibility: *Unchangeable Role*. Each user has a predefine role.

Privacy: *Existent*. To ensure security of SBB Direct Internet Banking System especially on protection of critical information and to guarantee secure transfer, several steps have been implemented

a) **Data Privacy, Confidentiality and Integrity**

In ensuring data transfer are not monitored, read or modified by unauthorized parties, Southern Bank's SBB Direct Internet Banking system has adopted a 128-bit encryption key to encrypt all the communication between the Bank's server and the client. They also have established a tight security procedure for their employees in handling all the devices that contain customers' data.

b) **Authentication**

Other than username and password identification, Southern Bank's SBB Direct Internet Banking system uses Digital certificates to identify the person who login on to the system.

c) **Non-Repudiation**

Pursuant to Southern Bank's SBB Direct Internet Banking terms and conditions, all transactions initiated with the customer's username and password shall be attributed to the customer and the Bank shall be entitled to carry out the transaction as if the instruction was given by the customer.

d) **Access Control and System Design**

Southern Bank's SBB Direct Internet Banking system is built based on a system developed by Security First Technology. The system is widely used by other online banks worldwide. The system has implemented a strict access mechanism in assigning users as well as system applications privileges to execute certain tasks.

The system also keeps detailed logs for audit purposes on all transactions executed as well as other activities such as log on / log off and any other enquiries.

As computer viruses are becoming a major threat to computers, the system has a detection mechanism that detects as well as removes not only computer viruses but also malicious codes, Trojan horse and any other hacking tools. It also logs all these activities for further analysis.

SBB has installed an Intrusion and Monitoring Detection mechanism on the network as well as on the servers. This mechanism is being monitored closely to analyze and detect any malicious attempt made to the system. To perform due diligence, they have engaged a third party to perform a penetration testing to identify, isolate and confirm any flaws on the system settings and configuration**.**

e) Operating System's Security Features

Southern Bank's SBB Direct Internet Banking uses a system that was developed as a multilevel security platform called Virtual Vault. It is the commercial version of Trusted Military Grade (Trusted) operating system. Virtual Vault provides a hierarchy of authorizations and privileges that protect the system's functions from outside interference by using a strictly partitioned Web runtime

environment and a securely integrated, industry leading web server.

The Trusted operating system replaces the concept of the root account in a traditional UNIX system with a privileged mechanism that allows individuals much less power and access than the root user identity. The system has explicit rules for granting privileges to specific processes. Those privileges provide the foundation for an authorization mechanism that controls user access to system functions.

The authorization mechanism limits a user's actions to the commands for which he has authorized. Unrecognized user or unfamiliar applications are not granted privileges, and therefore cannot gain access.

An information separation within the trusted operating system creates a wall between the network environment and the internal Bank applications. The network receives the user's request and validates his or her identity. A Trusted forwarding application then routes the request to the internal Bank environment, where it is processed and then passed back.

Because of this separation, nothing from the outside environment can touch the banking functions. Further, no outside processes can disrupt the internal operations of the Bank. This protects the Bank against any security breach occurring within the web server.

Divisibility: *No divisibility* because the payment system is notational systems.

Desirable Requisites

Integrity: *guaranteed*. Intrusion and Monitoring Detection.

Robustness: *Yes*

Economic Viability: *viable*

Scalability: *high*. The system is able to cope with the addition of new users and with the increase of the quantity of money involved in its operation without a significant loss of performance.

Interoperability: *no interoperability*. Technically, the system support interoperability but it is still cannot be implemented due to lack of policy to guarantee healthy competition among banks.

Auditability: *guaranteed*. The system provides auditing facilities so that errors or misuse may be detected. Other benefit of Virtual Vault operating system is its audit mechanism. The system records all suspicious activity, including the use of privilege, access violations, logins, logouts and unsuccessful network connections. This provides accountability for all internal procedures as well as attempted break-ins.

System Functionality Description

Establishment of Long Term Relationship: All Internet Banking customer need to visit any branch they have selected for the first time to make an initial deposit, sign the specimen signature card and collect their ATM Card and PIN. This is the policy endorsed by Bank Negara Malaysia.

Withdrawal: *none*

Transaction:

1. Authentication
2. Payment
3. Acknowledgement
4. Conclusion

Settlement: Bank deposit payee account and sent detail to payee.

Implementation Aspects

Cryptography: Southern Bank's SBB Direct Internet Banking uses SSL to implement the rapidly emerging technology of public key cryptography, used for client server authentication. As soon as it is readily available, this added level of security would be included in all banking transaction over the Internet.

The protection provided by SSL is sufficient to ensure confidentiality of customers' financial and personal data. Password violations do tend to increase over time, as the perpetrators have more opportunity to observe the workings of the network and the customers lose or otherwise compromise their passwords.

For this reason, security procedures will be frequently added to the Bank's applications as these new technologies become available.

Under public key cryptography, the Bank will issue the customer with a public/private key pair. The public key is a distributed number, the private key is known only to its owner. Messages encrypted using the public key can only be decrypted with the private key.

Key pairs are the perfect mechanism for mutual authentication, that is, each participant in a transaction can verify the identity of the other before proceeding.

To begin a transaction, the customer uses his or her browser to send a secure message via SSL to the Bank. The Bank responds by sending a certificate containing the Bank's public key. The browser authenticates the certificate, and then generates a new message containing the customer's public key, which is encrypted with the Bank's public key. The Bank uses its private key to decrypt this message, and sends its response to the customer encrypted with the customer's public key.

The browser uses the customer's private key to decrypt this message. In this way, the customer and the Bank can each authenticate the identity of the other. At this point, the browser generates a random session, or symmetric key, and encrypts it using the Bank's public key.

The Bank uses its private key to decrypt the symmetric key. The symmetric key is then used to encrypt all other data transferred in the current session. Session keys are unique for each communication with Southern Bank's SBB Direct Internet Banking, reducing the risk of anyone breaking into the transaction.

Network Connection: Further protection from intruders exists in Southern Bank's SBB Direct Internet Banking system of firewalls and filtering routers. Each presents an additional barrier between the Internet and the internal Bank network.

Filtering routers are used to verify the source and destination of each information packet sent to the Bank, and filter out all packets not addressed to specific network services. The filtering router eliminates any outside packets with an inside source address, to prevent outside users from trying to masquerade as internal sources. The only traffic allowed to the Bank's server is secure HTTP (HTTPS) traffic.

Firewalls work in a similar way, examining each packet of information that is sent across the Internet to the customer service network. The purpose of the firewall is to protect the Bank's internal network from outside observation. All traffic to the firewall is filtered and verified.

Payment order format: *N/A*

3. Hong Leong Bank Berhad – Hong Leong ec-Banking

Hong Leong ec-Banking service can be access through www.hlb.com.my.

System Typification

Exchange Model: *Notational*. Payment is done by the settlement of balances in accounts managed by the bank.

Central Authority Contact: *On-line*. The bank must be contacted during each transaction in order to verify all value transfers.

Payment Value: *Medium Payment*. System support value between RM1.00 and RM3000.

Hardware: *General Purpose*. Only common computers are needed.

Possible Roles: Bank, Customer, Merchant/Vendor

Role Inversibility: *Unchangeable Role*. Each user has a predefine role.

Privacy: *Existent*.

Divisibility: *No divisibility* because the payment system is notational systems.

Desirable Requisites

Integrity: *guaranteed*. To ensure data confidentiality and integrity, all information transmitted over the Internet is encrypted using the Secure Server Layer secured 40-bit from Verisign Certificate Authority

Robustness: *N/A*

Economic Viability: *N/A*

Scalability: *high*. The system is able to cope with the addition of new users and with the increase of the quantity of money involved in its operation without a significant loss of performance.

Interoperability: *no interoperability*.

Auditability: *guaranteed*. To provide a secured environment for ec-banking, HLB adopts a combination of system security and monitoring.

Internal System Audit as well as external security experts conducts regular security reviews on the systems.

System Functionality Description

Establishment of Long Term Relationship: Hong Leong ec-banking is eligible to all Internet users who are 18 years and above. To access to ec-banking, they need to have a Hong Leong Bank Phone Banking service either with ATM or credit card

Withdrawal: *none*

Transaction:

1. Authentication
2. Payment
3. Acknowledgement
4. Conclusion

Settlement: Bank deposit payee account and sent detail to payee.

Implementation Aspects

Cryptography: *N/A*

Network Connection: Firewall systems, strong data encryption, anti-virus protection and round the clock security surveillance systems to detect and prevent any form of illegitimate activities on network systems.

Payment order format: *N/A*

USE OF POCKETPC AS CLIENT DEVICE

Generally, 3COM Palm Pilot devices running its proprietary operating system known as the PalmOS, are dominating present market share for PDAs **[5]**. However there is an increase interest from other companies like Compaq, Casio and Hewlett Packard to compete with 3COM in the PDA's business market. The three main rivals of 3Com, instead of producing their own set of operating system for their PDAs, they are using Windows CE developed by Microsoft. Windows CE is a compact edition of the world-widely used Windows operating system and has recently been upgraded to version 3. The present growth of Windows CE is encouraging. Users whom are used to Windows and its supporting applications will find Windows CE is fairly similar and easy to use as Windows itself. Again the Windows CE front-end user interface has a more attractive appearance as compared to the PalmOS.

On April 2000, Microsoft unveiled their new handheld organizers call Pocket PC that is based on the latest version of Windows CE.

The use of PocketPC in this study is mainly because it's capability to browse the Internet via a Local Area Network, 56K modem or wireless solution. PocketPC user can now truly have universal access to their important Internet and intranet information at any time and any place. To lets user browse the World Wide Web, user of PocketPC can use Pocket Internet Explorer as their browser. PIE is an HTML 3.2 compatible web browser that supports the majority of web technologies such as tables, frames, secure sites, multiple fonts, images, and even Microsoft Jscript.

Briefly, the following is a list of web technologies that is supported by PIE:

1. HTML 3.2
2. Secure Socket Layer (SSL) version 2.0and 3.0 for secure transaction
3. Microsoft Jscript for scripting Web page behavior
4. Cookies
5. Frame (but not more than 2)
6. ActiveX Control
7. Extensible Markup Language (XML)
8. Background sound

The following is a list of web technologies that is not supported by PIE for now:

1. Cannot spawn multiple windows
2. Limit the use of frames to no more than 2
3. Animated GIF
4. VBScript
5. DHTML

6. CCS

We have conducted a study to determine whether Internet Banking website in each bank supports the use of PIE as client's browser. The first level of the study involves an interview with the officer in charge of the system of Internet Banking in each bank. List of web technology that is not supported by PIE was generated as a question of the interview. Here, we make an assumption that if one of the lists is fulfill then the customers of the particular bank cannot use PocketPC as their client's device.

Figure 2 shows the result. This shows that each bank uses at least one web technology that is not supported by PocketPC. The implication towards this finding is that PocketPC's user in Malaysia cannot use PocketPC correctly as a client device at Maybank2u.com, HLB ec-Banking and SBB Direct website.

Research is still on going to identify the best step on how the webmaster can offer the service of Internet Banking to Pocket PC user without involving total changes towards the existent website.

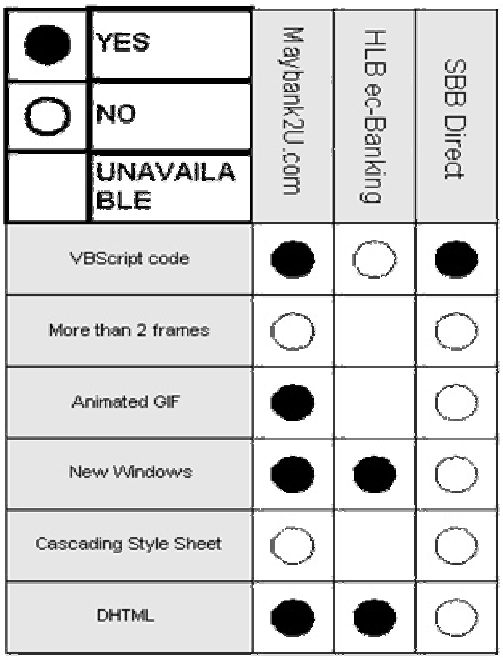

Figure 2 : Several web technology used in Internet Banking website

CONCLUSION

Most online delivery strategies to date have merely been to develop a website on which customers can engage with several financial transactions such as funds transfer, balance enquiry and the ability to see the past few transactions. Online delivery is, of course, not only about websites accessed via a PC, but the bank website should also consider other online devices – personal digital assistants, Wap-enable mobile phones, and even our interactive digital TV. This study also realizes that although the bank industry in Malaysia is ready with their IT infrastructure, it seems that confidence towards society's acceptance still very low. This will not encourage the bank to prepare better delivery channel considering the investment is very high.

REFERENCES

[1] Anonymous., 2001. "E-dagang Malaysia dijangka cecah RM35.7b." Utusan Malaysia, April 30, Megabait, 4

[2] Boneh, D., Daswani N., 1999. Experimenting with Electronic Commerce on the PalmPilot. Proceedings Eurocrypt '99 volume 1648 of Lecture Notes in Computer Science: 1-16

[3] *Put Your Site in the User's Pocket*, 2000. Internet: http://www.microsoft.com/mobile/developer/technicalarticles/pie_dev.asp

[4] L. de Carvalho Ferreira, R. Dahab. 1998. A scheme for analyzing electronic payment systems. Proceedings of the 14th Annual Conference on Computer Security Applications, IEEE: 137-146

[5] *Palm Slips, Pocket PC Gains In Europe*, 2001. Internet: http://www.allnetdevices.com/wireless/news/2001/05/09/palm_slips.html