PORTABLE HANDHELD SECURED ELECTRONIC BANK TO HOME SYSTEM

P.SUNEEL KUMAR, BALAGAM SIRISHA
Assistant Professor, M.TECH STUDENT
Dept of ECE,Megha Institute of Engineering & Technology For womens,Edulabad,Ghatkesar mandal,RangaReddy Dist,Telangana ,India

Abstract

To create a secured handheld 'doorstep banking' system called micro bank machine which is used to provide service to the customers in reserved areas and remote places. This is most important for physically challenged persons. The device completely operated in both online and offline mode. Implementation of this work to provide security purpose for user privacy in specific RFID application like location or location related information (speed) behaves as a legitimate access context. We show that both tags and back end server are used in location awareness for protecting against unauthorized reading and relay attacks on RFID system .location aware selective unlocking mechanism can be designed for which tags can selectively respond to reader interrogations rather than doing so promiscuously. In server side, location aware secure transaction verification scheme designed for bank server to decide whether to approve or deny a payment transaction and find a particular type of relay attack involving malicious readers.

Keywords: *RFID, location sensing, relay attack*

Introduction

Generally, ATM card connects directly with your bank account to give you access to your account through an automated teller machine. With the card, you can make deposits or withdrawals wherever you find an ATM at the bank, the mall or a grocery store. Learn specific disadvantages of using ATM services with your bank account to protect yourself from the downside of this convenience. Criminals target ATMs, so using an ATM could place you at risk for robbery after withdrawing money from the machine. Always choose an ATM in populated area to increase your safety during and after the transaction. If you lose your ATM card to theft and the thief has access to your account PIN, you may lose your account balance. Never write your PIN on anything that you carry with you because a thief could find both your ATM and the PIN to gain access to your account on most modern ATMs, the customer is identified by inserting a plastic ATM card with a

magnetic stripe or a plastic smartcard with a chip that contains a unique card number and some security information such as an expiration date. Authentication is provided by the customer entering a personal identification number (PIN).Using an ATM, customers can access their bank deposit or credit accounts in order to make a variety of transactions such as cash withdrawals, check balances, or credit mobile phones. If the currency being withdrawn from the ATM is different from that in which the bank account is denominated the money will be converted at an official exchange rate.

The scope of this work helps in reserved area people to get banking services such as cash deposit and cash withdrawal. It would save people time and money as they need not leave the place where they are. The system can also be operated

Within and beyond the normal banking hours. Offline mode is available to operate it in completely remote areas where even GSM communication is not available. Storage capacity of fingerprint scanner is in greater than 250. But can be extended to more than thousand if required. Panic button feature prevents a money theft from Business Correspondence (BC). Fig.1 shows the micro bank machine.

Figure 1.Microbank Machine

Because the machine is intended for reserved area, power will be not be easily available in remote places. So, the system operates with battery power. Low power 32-bit ARM Cortex-M3 microcontroller enables highly deterministic operation using battery power only. The colour display would help this process by rendering an onscreen touch keypad. Also increase the performance of the device and large onboard memory to store.

Background and Prior Work

In this paper, the existing counter measures against unauthorized reading and relay attacks. And also provide background information about current mobile payment system [1] which is susceptible to the reader and ghost relay attack.

Prior Work

Hardware based selective unlocking. Hardware-based selective unlocking schemes have been proposed previously.

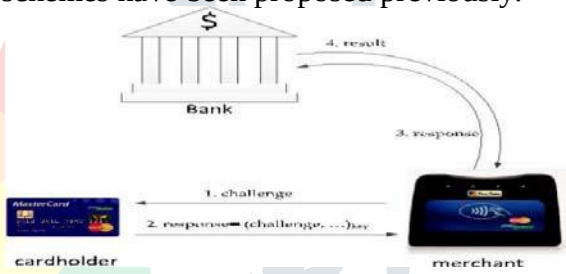

Figure 2. Online authorization in a mobile payment system

These include: Blocker Tag [10], RFID Enhancer Proxy [6], RFID Guardian [7], and Vibrate-to-Unlock [4]. All of these approaches, however, require the users to carry an auxiliary device. In Blocker Tag [10], a special RFID tag, called "blocker," is used to disrupt the identification process used by the reader to identify tags in proximity [10]. RFID Enhancer Proxy [6] and RFID Guardian [7] are special RFID-enabled devices that could be implemented in a PDA or cell phone. They are assumed to come with greater computation

capability and, thus, can perform more sophisticated interactions with readers, on behalf of tags, for various security purposes.

Mobile Payment Infrastructure

EMV, named after its creators, Europay, Master Cards, and Visa, is a global standard for debit and credit card payments. Payment systems based on EMV have been introduced across the world, known by a variety of different names such as "Chip and PIN" [5]. MasterCard Pay Pass is another EMV compatible "contactless" payment protocol. Fig. 2 presents a simplified version of the EMV-based mobile payment system with online verification. The system consists of three entities of interest: RFID-enabled payment card, the merchant, and the issuer bank, which issues the card. The payment card stores card details such as the credit card number, name of the owner, and expiration date. It also stores a symmetric key shared with its issuer bank. The point-of-sale (PoS) terminal at the merchant side is equipped with an RFID reader. A transaction starts with the merchant issuing a challenge to the payment card. The card calculates a cryptographic response based on the challenge and other information using the key shared with the issuer bank. It then transfers the response to the merchant terminal through the RFID communication interface. The response is next forwarded by the terminal to the issuer bank, which verifies the response and approves the transaction, if authentication is successful. Our proposed secure transaction verification based on location sensing can work under the current payment infrastructure.

Location Sensing

Several positioning technologies can be used to get location information. The most popular positioning technologies to get location information include the satellite based GPS , Wi-Fi based positioning system, and cellular network based positioning system[3]. Each of these positioning systems has its own favorable environment and performs much better than the others in terms of location estimation accuracy in most situations hence a combination of them may not make sense to improve the overall accuracy [2].

New PIN Entry Method

We present a new PIN entry method with an easier input procedure. Because it requires a user to perform far less mental tasks than the RRF method [9], it significantly reduces error probability and PIN entry time [8].

Figure 3. First stages for PIN '8325', where the pass-object is given as '○'

Our method consists of two stages, i.e., a pass-object setting stage and a PIN entry stage. In the first stage, the user is given a random array of ten familiar objects such as '○' and '▲' together with digits from 0 to 9. Then the user recognizes the symbol right below the first digit of his PIN, remembers it as the temporary 'pass-object' and touch 'OK.' Figure 2 shows an

example of this stage in a prototype implementation on a smart phone, where the PIN is '8325' and the pass-object is '○.'

(a) (b)

Figure 3. A sub stage where'3' is entered using the pass object 'o'

The PIN entry stage consists of three sub-stages to enter the second, third and fourth digits. In each sub-stage, the user is given again a random array of ten objects, and is requested to enter a PIN digit by rotating the object array and aligning the pass-object with the current PIN digit. For this task, the user can use two additional buttons ('Left' and 'Right').

Figure 3 shows the sub-stage to enter the second digit '3,' where Fig. 3(a) and Fig. 3(b) show the challenge given to the user and the user's correct response, respectively. The user locates○' 'right below '3' by touching 'Left' four times, and commits to his choice by touching 'OK.' The user repeats this task with the third and fourth digits of PIN.

We presented a new PIN entry method which is more resilient to SSA than the regular method and also more acceptable than the RRF method in terms of PIN entry time and error probability. Our method provides shoulder surfing resilience even if the whole authentication procedure is recorded by the attacker.

Cell Sense System

Cell Sense works in two phases: 1) an offline fingerprint construction phase and 2) an online tracking phase. During the offline phase, a probabilistic fingerprint is constructed, where the RSSI histogram for each cell tower at given locations in the area of interest is estimated.

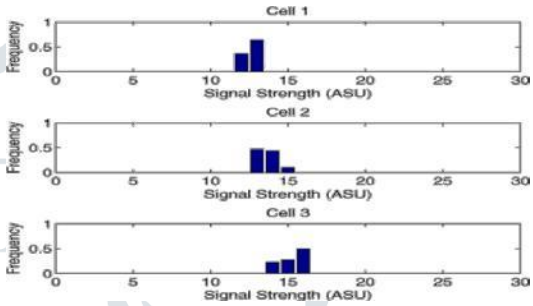

Figure 4. Example of the histograms from three adjacent cells from a certain cell tower.

This is performed in the Radio Map Builder module. Example of the histograms from three adjacent cells shows in Fig.4.

Working of Handheld Device

The main idea of handheld secured Electronic Doorstep Banking System is that the bank should employ special persons who are licensed as the business correspondents (BC) to carry a micro bank machine with them. Each BC will be allocated to a particular machine. The project and its security features along with the workflow will be described in a step by step manner in the following text. The customer who needs Bank service must call the customer care division of the bank and inform whether he wants to withdraw/deposit money. The bank server will choose the appropriate micro-bank unit and will send a query message to that. The

micro-bank machine should reply with an acknowledge message when it sees the bank query. The server will then dispatch a message about the details of the customer including his account balance. The message also contains a One-Time Password (OTP) to the micro-bank machine that is allocated for that transaction. The same OTP is also sent to the customer mobile. The micro-bank system is always connected to the central banking server using GSM communication.

The micro-bank machine that receives the OTP information will record the time of the arrival of this message. The machine internally runs a Real-Time-Clock (RTC) with battery backup which is derived from the satellite clock available in the received GPS data. The device has a built in high accuracy GPS unit to get precise time as well as accurate location information. A 3 hr transaction expiry period is set by default. This means the transaction should be completed within this timeframe, if not the device automatically cancels that particular transaction from proceeding further. This info will be sent to the server. The BC has to enter a touch screen password using the QVGA Touch screen TFT LCD Display in order to physically unlock the screen. The BC can unlock the screen anytime he wishes, but like a Smartphone, the screen will automatically get locked after a fixed (1 min) period of inactivity. Each micro-bank machine is permitted to be used only within a particular region in order to prevent an illegal usage out of that region and thus the device is locked in terms of its position. The current location of the device is tracked from GPS signals and the position is constantly verified with the region previously indicated by the server. This also helps to keep track of the location of the micro-bank machine in the event of misuse or a theft condition. An out of region condition brings the device to a halt and the error info is sent to the bank server.

On meeting the customer, the BC will verify the OTP on his device with that of the customer mobile. The customer needs to verify the OTP in his mobile against the micro-bank device. This mutual verification will authenticate both parties, and the transaction can now be started. The identity of BC is first verified using a built in Fingerprint Scanner. This is to ensure that the device has not been ended up in the wrong hands. The device stores the fingerprint of the BC as well as the entire customer base in that region in its database. Now the customer will be asked to enter his fingerprint. It is also verified. This ensures the authenticity of each party. Once the fingerprint verification is done, BC needs to enter a 4-PIN secret number on the touch screen keypad shown in the TFT display. The customer is then allowed to insert his smartcard into its slot. The device has a Smartcard Reader functionality that grabs the details such as the customer ID, customer name and account number information from the smartcard and will be verified against the server sent message. The smartcard is a permanent EEPROM memory that has got the customer details stored. Now it the customers turn to enter his 4-PIN secret number on the touch screen keypad [1], similar to that on the ATM machines. Once the PIN number is entered and verified, the machine will unlock the device for the final step in the

transaction. The customer will now be asked to enter the amount to be withdrawn on the touch screen display and the BC will dispatch the money to the customer. The figure 4 mentioned below described the working module.

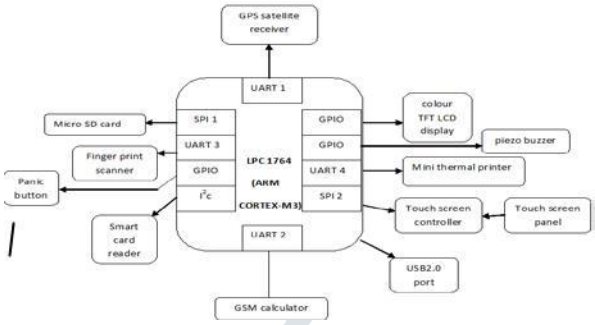

Figure 5. Block Diagram of Handheld Device

The customer must make a confirmation by typing the 4-PIN secret number again. The device checks this and sends a money paid message to the bank server. If the customer wants to deposit the money, he/she needs to enter the amount as previously described and the cash should be handed over to the BC. Now the BC will enter the 4-PIN secret number again.

Experimental Result Analysis

OUTPUT SCREENSHOT

Figure 6.Hardware Experimental setup of LPC1764 for off state

Future Enhancement

The customer who needs micro bank service must call the customer care division of the bank and inform whether he wants to withdraw/deposit money. The bank server will choose the appropriate BC and will send a query message to that. The micro-bank machine should reply with an acknowledge message when it sees the bank query. The server will then dispatch a message about the details of the customer including his account balance. The message also contains a onetime password to the micro-bank machine that is allocated for that transaction. The same OTP is also sent to the customer mobile. The micro-bank system is always connected to the central banking server using GSM communication. The micro-bank machine that receives the OTP information will record the time of the arrival of this message. The machine internally runs a Real Time Clock (RTC) with battery backup which is derived from the satellite clock available in the received GPS data. The device has a built in high accuracy GPS unit to get precise time as well as accurate location information. A 3 hr transaction expiry period is set by default. This means the transaction should be completed within this timeframe, if not the device automatically cancels that particular transaction from proceeding further. This info will be sent to the server. On meeting the customer, the BC will verify the OTP on his device with that of the customer mobile. This mutual verification will authenticate both parties, and the transaction can now be started.

Scope of the Study

This project ensures that provide the secured service to the customer in reserved area and remote places with the help of secured handheld doorstep bank machine. The feasibility of the system in terms of both technical and economical aspects.

Conclusion

The system has low Energy consumption, large communication range and high security characteristics. Handheld device can be extended to support multiple uses. Offline mode is available to operate it in completely remote areas where even GSM communication is not available and also support for uneducated people with money translation feature.

References

[1]Di Ma, Member, IEEE, Nitesh Saxena, Member, IEEE, Tuo Xiang, and Yan Zhu, "Enhancing RFID Security and Privacy via Location Sensing" March/April 2013

[2]D. Schon, H. Lemelson, and W. Effelsberg, "Situation-Aware Choice of the Most Accurate Positioning System," Proc. IEEE Int'l Conf. Pervasive Computing Comm. Workshops (PerCom '12), 2012.

[3]Mohamed Ibrahim, Student Member, IEEE, and Moustafa Yusuf, Senior Member, IEEE, An Accurate Energy Efficient GSM Positioning System"Janauary 2011.

[4]N. Saxena, B. Uddin, J. Voris, and N. Asokan, "Vibrate-to-Unlock: Mobile Phone Assisted User Authentication to Multiple Personal RFID Tags," Proc. IEEE Int'l Conf. Pervasive Computing and Comm. (PerCom), 2011.

[5]S. Drimer and S.J. Murdoch, "Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks," Proc. 16th USENIX Security Symp., Aug. 2007.

[6]A. Juels, P.F. Syverson, and D.V. Bailey, "High-Power Proxies for Enhancing RFID Privacy and Utility," Proc. Fifth Int'l Conf. Privacy Enhancing Technologies, 2005.

[7]M.R. Rieback, B. Crispo, and A.S. Tanenbaum, "RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management,"Proc. Australasian Conf. Information Security and Privacy (ACISP),2005.

[8]Chang Soon Kim, Mun Kyu Le, "Secure and user friendly PIN Entry method'' School of Computer and Information Engineering, Inha University, Incheon 402-751, Korea, October 2004.

[9]V. Roth, K. Richter, R. Freidinger, "A PIN-Entry Method Resilient Against Shoulder Surfing," ACM CCS'04, pp. 236-245, October, 2004.

[10]A. Juels, R.L. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," Proc. ACM Conf. Computer and Comm.