Transaction using Multiaccount Embedded ATM Card

Apeksha B M
Department of Electronics and Communication
Coorg Institute Of Technology, Ponnampet.

Prarthana M B
Department of Electronics and Communication
Coorg Institute Of Technology, Ponnampet.

Dechamma Pavan C
Department of Electronics and Communication
Coorg Institute Of Technology, Ponnampet.

Sithara Chondamma
Department of Electronics and Communication
Coorg Institute Of Technology, Ponnampet.

***Abstract*- The idea behind this work is that to add more then one bank account in an ATM card, so that the user need not carry more cards with them and complication of handling passwords. Here in this one we embedded more then one bank account so that the user can transact as she/he wish with a swipe. In addition to this convivence factor provided by multiaccount ATM we also provide enhance security features. Every time a card is swiped the user is intimated with a help of a GSM module. The GSM module sensor SMS to the user asking him/her to set a password of his/her choice. The same, registered password is to be entered through keypad and the amount is provided only if both the passwords match. The system also provides an option of choosing between several banks. The user can select which bank he desires to perform truncation with. This selection of choice is enabled by programming the keypad.**

Keywords— ATM, banks, fingerprint, smartcard, user authentication, PIN, transaction.

I. INTRODUCTION

In most modern ATMs, the customer identifies him or herself by inserting a plastic card with magnetic strip or plastic smart card with a chip that contains his or her account number. The customer then verifies his or her identity by entering a pass code (i.e.) personal identification number (PIN) of four digits. If the number is entered incorrectly several times consecutively (usually three), most ATMs will retain the card as a security precaution to prevent an unauthorized user from discovering the PIN by guesswork and so on. Moreover, there is a limitation in transaction for the other bank customers in using the ATM of some other bank crossing the limit they have to pay transaction fees. At present every customer has an individual ATM card for each and every bank in which he/she maintains account. So, handling the cards, their passwords play a major role here. So to overcome these difficulties we embedded more than one bank account of the user in a single ATM smart card, so that the user can swipe the card and can select the bank from which he/she are interested to carry out transaction.

II. OBJECTIVES

- Reduces the complexity of managing more than one ATM card and their passwords.
- Each time, the customer can change the password at the beginning of the transaction, thereby increasing the security.
- Every transaction that takes place will be authorized by the account holder through SMS.
- Cloud Computing concept for connecting respective bank ATM server.

III. SURVEY OF LITERATURE

In this chapter, we briefly explain about the current existing systems, the problems that are present in them and we also present various solution to overcome those problems and how we adopted these solutions into our project.

A. Multi Account Embedded ATM Card:

In the existing system, every customer has an individual ATM card for each and every bank in which he/she maintains account. So, handling the cards, their passwords play a major role here. So to overcome these difficulties we propose a system to embed more than one bank account of the user in a single ATM smart card, so that the user can swipe the card and will be able to select the bank from which he/she is interested to make a transaction [1].

In the existing ATM system all ATM machines are connected to their respective bank servers and all bank servers are connected to a single interface i.e. National Finance Switch (NFS). When the user swipes his ATM card at the respective bank's ATM machine, then that ATM machine directly links to its bank server for validation of ATM card. If the ATM card is of the same bank then transaction proceeds else connects to the respective bank's server via NFS for the further transaction.

B. Secure PIN Entry Method:

Personal identification number (PIN) is a common method to authenticate a user for various devices including automatic teller machines (ATMs), mobile phones, and so on. However, if someone observes the input procedure by using a tiny camera, he can easily get the PIN. This kind of attack is called 'shoulder surfing attack (SSA). We presenting new pin entry method, it contains two part that is four digits with one symbol which is given by user of the account. We adopt a completely different approach to

the existing problem and present a secure and practical PIN entry method. According to our experiments, the proposed method significantly reduces the error probability. The principal idea behind this method is each time user can set new password instead of bank and to avoid the card blocking procedure taken up by the banks if the user enters the wrong password more than three times [2].

C. *Real Time SMS-Based Security:*

Existing measures adopted by financial institutions require ATM card holders to optionally subscribe to financial transactions message alerts through Short Message Services (SMS) (debit and credit transactions) and the use of posters pasted in banking halls to warn customers on the need to protect PIN numbers from unauthorized users. These measures are purely informative and do not adequately deal with the problems in real time. In this project, we introduce a Real Time Instructive SMS-Based scheme called MophTem (Mobile phone Text message) scheme which compels all customers to subscribe to SMS alerts as a basis for initiating transactions on their account.

Every time the user's account is accessed, a message will be sent to the registered mobile number to authorize the transaction. Only after the user's confirmation is received, the transaction is processed [3].

D. *Cloud Based ATM Environment*

Cloud computing is a key technology to provide security for any advanced systems. In the scenario we are depicting, we leverage the use of the Cloud technology to reproduce real world scenarios encompassing distributed systems, e.g., several ATM centers belonging to the same system and deployed over different cities. we propose the adoption of a Private Cloud Infrastructure model to build up an advanced ATM system that will replace the existing systems by overcoming the problems which are there in the current systems and then to apply proposed methodology, after assessing the vulnerabilities of the system [4]. We propose a new cloud computing service called Data Protection as a Service.

Using this concept, we are concentrating on user authentication, data protection, and security parts. For the security in storage most system uses data protection mechanisms. They include graphical password, alphanumeric password and many other used similar ways that will help us to increase the security of data. In this system using cloud concept we are showing different banks in ATM system, it will contain many banks and we considered each bank as one cloud and it contains many user accounts of that bank.

IV. ARM LPC2148 MICROCONTROLLER

A. *Description*

The LPC2141/42/44/46/48 microcontrollers are based on a 16-bit/32-bit ARM7TDMI-S CPU with real-time emulation and embedded trace support, that combine microcontroller with embedded high-speed flash memory ranging from 32 kB to 512 kB. A 128-bit wide memory interface and unique accelerator architecture enable 32-bit code execution at the maximum clock rate. For critical code size applications, the alternative 16-bit Thumb mode reduces code by more than 30 % with minimal performance penalty.

Due to their tiny size and low power consumption, LPC2141/42/44/46/48 are ideal for applications where miniaturization is a key requirement, such as access control and point-of sale. Serial communications interfaces ranging from a USB 2.0 Full-speed device, multiple UARTs, SPI, SSP to I2C-bus and on-chip SRAM of 8 kB up to 40 kB, make these devices very well suited for communication gateways and protocol converters, soft modems, voice recognition and low-end imaging, providing both large buffer size and high processing power. Various 32-bit timers, single or dual 10-bit. ADC(s), 10-bit DAC, PWM channels and 45 fast GPIO lines with up to nine edge or level sensitive external interrupt pins make these microcontrollers suitable for industrial control and medical systems.

B. *Features*

- 16-bit/32-bit ARM7TDMI-S microcontroller in a tiny LQFP64 package.
- 8 kB to 40 kB of on-chip static RAM and 32 kB to 512 kB of on-chip flash
- memory. 128-bit wide interface/accelerator enables high-speed 60 MHz operation.
- In-System Programming/In-Application Programming (ISP/IAP) via on-chip boot
- loader software. Single flash sector or full chip erase in 400 ms and programming of 256 bytes in 1 ms.
- Embedded ICE RT and Embedded Trace interfaces offer real-time debugging with the on-chip Real Monitor software and high-speed tracing of instruction execution.
- USB 2.0 Full-speed compliant device controller with 2 kB of endpoint RAM. In addition, the LPC2146/48 provides 8 kB of on-chip RAM accessible to USB by DMA.
- One or two (LPC2141/42 vs. LPC2144/46/48) 10-bit ADCs provide a total of 6/14 analog inputs, with conversion times as low as 2.44 µs per channel.
- Single 10-bit DAC provides variable analog output (LPC2142/44/46/48 only).
- Two 32-bit timers/external event counters (with four captures and four compares channels each), PWM unit (six outputs) and watchdog.
- Low power Real-Time Clock (RTC) with independent power and 32 kHz clock input.
- Multiple serial interfaces including two UARTs (16C550), two Fast I2C-bus (400 Kbit/s), SPI and SSP with buffering and variable data length capabilities.
- Vectored Interrupt Controller (VIC) with configurable priorities and vector addresses.
- Up to 45 of 5 V tolerant fast general purpose I/O pins in a tiny LQFP64 package.
- Up to 21 external interrupt pins available.
- 60 MHz maximum CPU clock available from programmable on-chip PLL with Settling time of 100 µs.
- On-chip integrated oscillator operates with an external crystal from 1 MHz to 25 MHz
- Power saving modes include Idle and Power-down.

- Individual enable/disable of peripheral functions as well as peripheral clock scaling for additional power optimization.
- Processor wake-up from Power-down mode via external interrupt or BOD.
- Single power supply chip with POR and BOD circuits:
- CPU operating voltage range of 3.0 V to 3.6 V (3.3 V ± 10 %) with 5 V tolerant I/O pads.

C. Functional Description

The ARM7TDMI-S is a general purpose 32-bit microprocessor, which offers high performance and very low power consumption. The ARM architecture is based on Reduced Instruction Set Computer (RISC) principles, and the instruction set and related decode mechanism are much simpler than those of micro programmed Complex Instruction Set Computers (CISC). This simplicity results in a high instruction throughput and impressive real-time interrupt response from a small and cost-effective processor core.

Pipeline techniques are employed so that all parts of the processing and memory systems can operate continuously. Typically, while one instruction is being executed, its successor is being decoded, and a third instruction is being fetched from memory.

The ARM7TDMI-S processor also employs a unique architectural strategy known as Thumb, which makes it ideally suited to high-volume applications with memory restrictions, or applications where code density is an issue. The key idea behind Thumb is that of a super-reduced instruction set.

The ARM7TDMI-S processor has two instruction sets:

- The standard 32-bit ARM set.
- A 16-bit Thumb set.

The Thumb set's 16-bit instruction length allows it to approach twice the density of standard ARM code while retaining most of the ARM's performance advantage over a traditional 16-bit processor using 16-bit registers. This is possible because Thumb code operates on the same 32-bit register set as ARM code. Thumb code is able to provide up to 65 % of the code size of ARM, and 160 % of the performance of an equivalent ARM processor connected to a 16-bit memory system. The particular flash implementation in the LPC2141/42/44/46/48 allows for full speed execution also in ARM mode. It is recommended to program performance critical and short code sections (such as interrupt service routines and DSP algorithms) in ARM mode. The impact on the overall code size will be minimal but the speed can be increased by 30% over Thumb mode.

D. On-chip Flash Memory

The LPC2141/42/44/46/48 incorporates a 32 kB, 64 kB, 128 kB, 256 kB and 512 kB flash memory system respectively. This memory may be used for both code and data storage. Programming of the flash memory may be accomplished in several ways. It may be programmed In System via the serial port. The application program may also erase and/or program the flash while the application is running, allowing a great degree of flexibility for data storage field firmware upgrades, etc. Due to the architectural solution chosen for an on-chip boot loader, flash memory available for user's code on LPC2141/42/44/46/48 is 32 kB, 64 kB, 128 kB, 256 kB and 500 kB respectively. The LPC2141/42/44/46/48 flash memory provides a minimum of 100,000 erase/write cycles and 20 years of data-retention.

E. On-Chip Static RAM

On-chip static RAM may be used for code and/or data storage. The SRAM may be accessed as 8- bit, 16-bit, and 32-bit. The LPC2141, LPC2142/44 and LPC2146/48 provide 8 kB, 16 kB and 32 kB of static RAM respectively. In case of LPC2146/48 only, an 8 kB SRAM block intended to be utilized mainly by the USB can also be used as a general-purpose RAM for data storage and code storage and execution.

F. Interrupt Controller

The Vectored Interrupt Controller (VIC) accepts all of the interrupt request inputs and categorizes them as Fast Interrupt Request (FIQ), vectored Interrupt Request (IRQ), and non-vectored IRQ as defined by programmable settings. The programmable assignment scheme means that priorities of interrupts from the various peripherals can be dynamically assigned and adjusted. Fast interrupt request (FIQ) has the highest priority. If more than one request is assigned to FIQ, the VIC combines the requests to produce the FIQ signal to the ARM processor. The fastest possible FIQ latency is achieved when only one request is classified as FIQ, because then the FIQ service routine does not need to branch into the interrupt service routine but can run from the interrupt vector location. If more than one request is assigned to the FIQ class, the FIQ service routine will read a word from the VIC that identifies which FIQ source(s) is (are) requesting an interrupt. Vectored IRQs have the middle priority. Sixteen of the interrupt requests can be assigned to this category. Any of the interrupt requests can be assigned to any of the 16 vectored IRQ slots, among which slot 0 has the highest priority and slot 15 has the lowest. Non-vectored IRQs have the lowest priority. The VIC combines the requests from all the vectored and non-vectored IRQs to produce the IRQ signal to the ARM processor. The IRQ service routine can start by reading a register from the VIC and jumping there. If any of the vectored IRQs are pending, the VIC provides the address of the highest priority requesting IRQs service routine, otherwise it provides the address of a default routine that is shared by all the non-vectored IRQs. The default routine can read another VIC register to see what IRQs are active.

G. *Interrupt sources*

Each peripheral device has one interrupt line connected to the Vectored Interrupt Controller but may have several internal interrupt flags. Individual interrupt flags may also represent more than one interrupt source.

V. PIN CONTROL BLOCK

The pin connect block allows selected pins of the microcontroller to have more than one function. Configuration registers control the multiplexers to allow

connection between the pin and the on-chip peripherals. Peripherals should be connected to the appropriate pins prior to being activated, and prior to any related interrupt(s) being enabled. Activity of any enabled peripheral function that is not mapped to a related pin should be considered undefined. The Pin Control Module with its pin select registers defines the functionality of the microcontroller in a given hardware environment. After reset all pins of Port 0 and 1 are configured as input with the following exceptions: If debug is enabled, the JTAG pins will assume their JTAG functionality; if trace is enabled, the Trace pins will assume their trace functionality. The pins associated with the I2C0 and I2C1 interface are open drain.

VI. FAST GENERAL-PURPOSE PARALLEL I/O (GPIO)

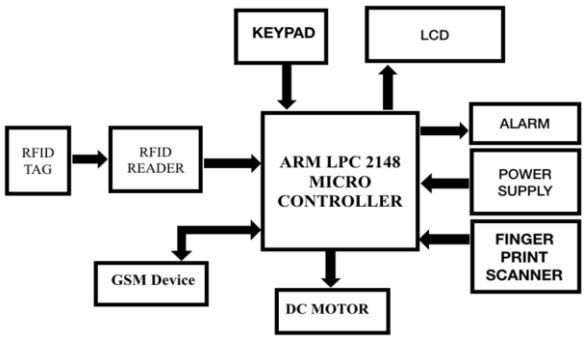
Device pins that are not connected to a specific peripheral function are controlled by the GPIO registers. Pins may be dynamically configured as inputs or outputs. Separate registers allow setting or clearing any number of outputs simultaneously. The value of the output register may be read back, as well as the current state of the port pins. LPC2141/42/44/46/48 introduce accelerated GPIO functions over prior LPC2000 Devices:

- GPIO registers are relocated to the ARM local bus for the fastest possible I/O timing.
- Mask registers allow treating sets of port bits as a group, leaving other bits unchanged.
- All GPIO registers are byte addressable.
- Entire port value can be written in one instruction

A. Features

- Bit-level set and clear registers allow a single instruction set or clear of any number of bits in one port.
- Direction control of individual bits. • Separate control of output set and clear.
- All I/O default to inputs after reset.

VII. BLOCK DIAGRAM



VIII. WORKING

- Wireless scanning of ATM cards.
- Authentication using Fingerprint
- Sending password request SMS to user when fingerprint recognition failed
- Waiting for reply from user
- If no reply comes transaction is blocked
- If there is a password reply goes for bank selection.
- Selecting a required bank service using the display
- Ask for password entry
- Comparison of entered and sent password
- If both are matching go for transaction
- Send a confirmation message to user
- If the PIN entered is wrong for three consecutive times, there will be a buzzer and then the transaction is cancelled.

IX. FUTURE OF SCOPE

- Can be implemented on existing ATM systems.
- We can embed a biometric scan in the smart card i.e. multi component card.
- This project can be implemented for office security, colleges, and hospitals and also in parking system.

X. CONCLUSION

Thus, the user can manage his/her multiple accounts in various banks with the help of this single smart card which provides easy access. Reduces the complexity of managing more than one ATM card and their passwords. Leads to avoiding transaction charges levied on the users/ customers for transactions done in ATMs other than their respective banks. Production cost of ATM cards can be reduced.

REFERENCES

[1] Gokul.r, Godwin Rose Samuel.W, Arul.M, Sankari.C" Multi Account Embedded ATM Card", International Journal of Scientific and Engineering Research, Volume, Issue 4 APRIL 2013, ISSN 2229-5518

[2] Chang Soon Kim, Mun-Kyu Lee" Secure and User Friendly PIN Entry Method", IEEE, Incheon 402-751, 2010

[3] Ugochukwu Onwudebelu, Olumide Longe, Sanjo Fasola, Ndidi C. Obi and Olumuyiwa B. Alaba "Real Time SMS-Based Hashing Scheme for Securing Financial Transactions on ATM Systems ", 3rd IEEE International Conference on Adaptive Science and Technology 2011

[4] Antonio Marotta, Gabriella Carrozza, Luigi Battaglia, Patrizia Montefusco, Vittorio Manetti SESM S.C.A.R.L, "Applying the SecRAM Methodology in a Cloud-based ATM Environment " IEEE International Conference on Availability, Reliability and Security,2013

[5] Harshal M. Bajad1Sandeep E. Deshmukh Pradnya R. Chaugule Mayur S. Tambade "Universal ATM Card System", International Journal of Scientific and Engineering Research, Volume 1, Issue 8 OCTOBER 2012, ISSN 2278-0181

[6] Philip K. Chan, Wei Fan "Disfribufed Dam Mining in Credit Cud Fmud Defwdon" IEEE, NOVEMBER/DECEMBER 1999

[7] Sebastien Jean, Didier Donsez, Sylvain Lecomte "Using Some Database Principles to Improve Cooperation in Multi-Application Smart Cards" IEEE, JULY 2001.

[8] Ling-Yu Duan. Xiao-Dong Yu, Qi Tian ,Qibin Sun "Face pose analysis from mpeg compressed video for surveelance applications"IEEE, MARCH 2003

[9] Vinod Chcrian Joseph, Kyung Hee Lee, Doohyun Kim, Sung Ho Ahn, Ji-Young Kwak "Embedded ATM Access Point: Optimal Design at Food Court" IEEE 10th Asia-Pacific Conference on Communication and 5th International Symposium on Multi-Dimensional Mobile Commnications, SEPTEMBER 2004

[10] Jae Hyung Joo, Jeong-Jun Suh, and Young Yong Kim, "Secure Remote Usim(Universal Subscriber Identity Module) Card Application Management Protocol For W-Cdma Networks" IEEE,APRIL 2006