ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue.2 April 2024

SMS based Banking security system

Jadapally Chandra Shekar [1], Saripella Srikanth Sai Varma [2],
Bikkireddy Abhi Ram Reddy[3], Biyyala Vasudev [4],
Mr. P. Venkatapathi[5]
[1,2,3,4] UG Student, Dept. of ECE, CMR Institute of Technology, Hyderabad
[5] Assistant Professor, Dept. of ECE
CMR Institute of Technology, Hyderabad

Abstract

Bank locker security is important for everyone. Many times we forgot to carry the key of our bank locker. In these cases it is really difficult to open the locker. This project is designed to solve this purpose. Main concept behind this project is of a bank locker-latch opening using two passwords entered through SMS and keypad. Each bank locker will have a GSM modem connected to it. When owner of the bank locker wants to open the locker then he/she has to sends a password through SMS. Then microcontroller connected to GSM modem reads the contents of password. If contents are correct then it will enable the keypad to enter second password. Now user has to enter second password using Keypad. If second password is correct then system allows user to access locker. We have provided a DC motor which will operate when both passwords are correct. Buzzer will be turned on if any one of two password is wrong. Microcontroller sends SMS to user for wrong password as well as for correct password. We have also provided an Infrared sensor in this project. Infrared sensor will be triggered when some person is standing in front of Locker. Then system will send SMS to the owner. This is low warning message as, “Some person is standing in front of your bank locker”. IR sensor will be turned off when user send first password through SMs

INTRODUCTION

M-banking system is one which provides all daily banking operations to customer with one click of his mobile handset with supported application. M-banking system has potential to provide access or delivery of very specific and highly necessary information to customer as given in [2]. Growth in the M-Banking is driven by various facilities like convenience of banking operations, greater reach to consumers and Integration of other m-commerce services with mobile banking. In M-banking there is no place restriction, it is highly penetration coefficient as growth of mobile phones are more than computers, it is fully personalized and private increasing transaction authenticity and is 100% available all the time with users. However, there are several challenges that need to be addressed to completely utilize the benefits of the M-Banking like handset compatibility, security, scalability, reliability. Due to increase in use of mobile handsets for many m-commerce applications, Chances of mobile hacking for financial benefits are heavily increased. Currently mostly all banks in India and outside are sending text SMS directly to the customer handset for basic bank services without any security which can be accessed by any malicious person and can use this information for getting access to customer account. OTA (Over-the-air) mobile data can be hacked in network path from bank to customer mobile handset including MPIN, a password use for user identification in M-banking. Thus there is a need of secure and cost effective solution which can be easily provided on all types of handsets. Our objective is to provide cost effective, secure, fast M-banking solution combining features of cryptography.

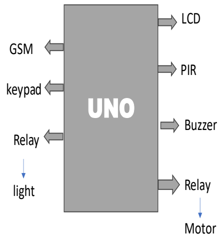
EXISTING SYSTEM

Even though various channels are available for M-banking most of the banks uses SMS as basic and cheap channel for basic banking operations. Currently all banks in India like ICICI, HSBC, SBI etc are not using any encryption techniques in SMS based M-banking system. They are using simple text based SMS for customer queries in which they directly send account information to customer only hiding some digits of account number which can be easily hacked by any hacker or seen by anyone from message inbox. Even though some banks do provide some other channel like GPRS and WAP but cost of implementation is more and these facilities are not available on all types of mobile handset thus there is a need of secure and cost effective solution which can be easily provided on all types of handsets.

PROPOSED SYSTEM

Current real time M-banking application of various banks uses plain text messages without any security algorithm for sending data in SMS banking hence any malicious user can access customer important data on mobile. Proposed secure M-banking is based on symmetric cryptographic techniques where common secret key is shared among bank customer and bank server. Proposed Architecture consists of 4 components as Customer Mobile application, Bank Server application, Bank side mobile / GSM Modem, Bank database and wireless OTA [1]. Our solution uses windows mobile as client application platform and .NET framework as server side software. Customer interested in using M-Banking facilities has to make registration only once with corresponding bank. Bank has all necessary details of customer in database. Bank sends Customer–side mobile application developed for windows mobile to user. Application will be installed once on windows mobile supported handset. This application consists of Login screen along with get session key option, menu screen for bank services options, and encryption and decryption screens for outgoing and incoming secure SMS and send message screen to send SMS to server GSM handset /Modem. Application will be updated as and when bank updates it.

Block diagram



ARUDINO:

The Arduino is a family of microcontroller boards to simplify electronic design, prototyping and experimenting for artists, hackers, hobbyists, but also many professionals. People use it as brains for their robots, to build new digital music instruments, or to build a system that lets your house plants tweet you when they're dry. Arduinos (we use the standard Arduino Uno) are built around an ATmega microcontroller — essentially a complete computer with CPU, RAM, Flash memory, and input/output pins, all on a single chip. Unlike, say, a Raspberry Pi, it's designed to attach all kinds of sensors, LEDs, small motors and speakers, servos, etc. directly to these pins, which can read in or output digital or analog voltages between 0 and 5 volts. The Arduino connects to your computer via USB, where you program it in a simple language (C/C++, similar to Java) from inside the free Arduino IDE by uploading your compiled code to the board. Once programmed, the Arduino can run with the USB link back to your computer, or stand-alone without it — no keyboard or screen needed, just power.

PIR SENSOR

PIR Sensor is short for passive infrared sensor, which applies for projects that need to detect human or particle movement in a certain range, and it can also be referred as PIR(motion) sensor, or IR sensor. Since its powerful function and low-cost advantages, it has been adopted in tons of projects and widely accepted by the open-source hardware community for projects related to Arduino and raspberry pi. All this can help the beginners learn about PIR sensor more easily.

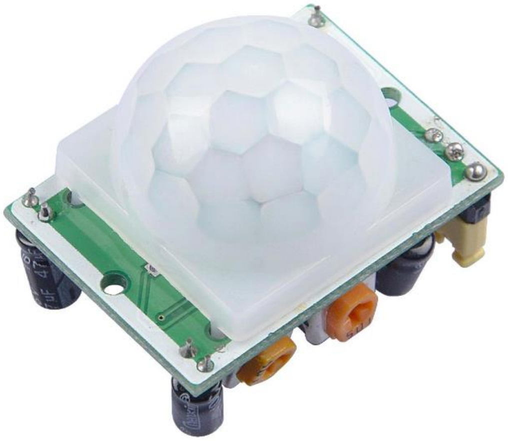


Image: PIR Motion Sensor – Large Lens version

BUZZERS

In common parlance a Buzzer is a signaling device that is not a loudspeaker. It can be mechanical, electromechanical, or electronic (a piezo transducer). BeStar produces Buzzers in every available configuration for a wide variety of applications. A Piezo transducer can produce the sound for panel mount buzzers, household goods, medical devices and even very loud sirens. When a lower frequency is required an electromagnetic buzzer can fill the need. These are very common in automotive chimes and higher end clinical diagnostic devices. The BeStar buzzer range includes self drive units with their own drive circuitry (indicators), or external drive units, which allow the designer the flexibility to create their own sound patterns.

GSM (Global System for Mobile communications)

GSM (Global System for Mobile communications) is a cellular network, which means that mobile phones connect to it by searching for cells in the immediate vicinity. GSM networks operate in four different frequency ranges. Most GSM networks operate in the 900 MHz or 1800 MHz bands. Some countries in the Americas use the 850 MHz and 1900 MHz bands because the 900 and 1800 MHz frequency bands were already allocated. The rarer 400 and 450 MHz frequency bands are assigned in some countries, where these frequencies were previously used for first-generation systems.

GSM-900 uses 890–915 MHz to send information from the mobile station to the base station (uplink) and 935–960 MHz for the other direction (downlink), providing 124 RF channels (channel numbers 1 to 124) spaced at 200 kHz. Duplex spacing of 45 MHz is used. In some countries the GSM-900 band has been extended to cover a larger frequency range. This 'extended GSM', E-GSM, uses 880–915 MHz (uplink) and 925–960 MHz (downlink), adding 50 channels (channel numbers 975 to 1023 and 0) to the original GSM-900 band. Time division multiplexing is used to allow eight full-rate or sixteen half-rate speech channels per radio frequency channel. There are eight radio timeslots (giving eight burst periods) grouped into what is called a TDMA frame. Half rate channels use alternate frames in the same timeslot. The channel data rate is 270.833 kbit/s, and the frame duration is 4.615 ms.

CONCLUSION

We have implemented a secure SMS based Mobile Banking system. The system allows user to carry out all banking transaction securely from anywhere, anytime. All messages from user windows mobile are sent in encrypted format to bank server. Bank server decrypt message, process query and encrypt result in SMS. Server sends message to customer which will be decrypted on his handset. The evaluation of the system was studied for varying banking transaction and under various security threatening malicious activities were recorded. Performance of the transaction is studied. We have executed few banking transaction from HTC windows mobile and using VB.Net server side application. We have used LG GSM mobile as server attached mobile device. Experiments shows that secure SMS Mobile banking provides cost effective and secure system with satisfying Confidentiality, Authentication, Integrity and Non-Repudiation using symmetric cryptography. Application can be used on any windows mobile supported handset from anywhere as no GPRS and WAP are required. We have implemented system using symmetric key AES algorithm. In future better power consumption algorithm like blowfish can be tried out. Steganogrpahy can also be applied for secure M-banking transactions. We can use concept of STK, SIM application toolkit where bank can stored the application and encryption keys on SIM.

REFERENCES

[1] Mohammad Shirali-Shahreza and M. Hassan Shirali-Shahreza, “Mobile banking Services in bank area”, SICE Annual Conference 2007, Japan

[2] Martinez Borreguero, F. Javier and Chaparro Peláez, Julián,”Spanish Mobile Banking Services: An Adoption Study”, Proceedings of the International Conference on Mobile Business 2005.

[3] Mohammad Shirali-Shahreza,”Improving Mobile Banking Security Using Steganography “, International Conference On Information Technology.

[4] Przemyslaw Krol, Przemysław Nowak, Bartosz Sakowicz,”Mobile Banking Services Based On J2ME/J2EE”, CADSM’2007.

[5] Yousuf S. AlHinai, Sherah Kurnia and Robert B. Johnston,”Adoption of Mobile, Commerce Services by Individuals: A Meta-Analysis of the Literature”, Sixth International Conference on the Management of Mobile Business .

[6] Karne, R. K. ., & Sreeja, T. K. . (2023). PMLC- Predictions of Mobility and Transmission in a Lane-Based Cluster VANET Validated on Machine Learning. International Journal on Recent and Innovation Trends in Computing and Communication, 11(5s), 477–483. https://doi.org/10.17762/ijritcc.v11i5s.7109

[7] Radha Krishna Karne and Dr. T. K. Sreeja (2022), A Novel Approach for Dynamic Stable Clustering in VANET Using Deep Learning (LSTM) Model. IJEER 10(4), 1092-1098. DOI: 10.37391/IJEER.100454.

[8] Reddy, Kallem Niranjan, and Pappu Venkata Yasoda Jayasree. "Low Power Strain and Dimension Aware SRAM Cell Design Using a

New Tunnel FET and Domino Independent Logic." International Journal of Intelligent Engineering & Systems 11, no. 4 (2018).

[9] Reddy, K. Niranjan, and P. V. Y. Jayasree. "Design of a Dual Doping Less Double Gate Tfet and Its Material Optimization Analysis on a 6t Sram Cells."

[10] Reddy, K. Niranjan, and P. V. Y. Jayasree. "Low power process, voltage, and temperature (PVT) variations aware improved tunnel FET on 6T SRAM cells." Sustainable Computing: Informatics and Systems 21 (2019): 143-153.

[11] Reddy, K. Niranjan, and P. V. Y. Jayasree. "Survey on improvement of PVT aware variations in tunnel FET on SRAM cells." In 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), pp. 703-705. IEEE, 2017