International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.01, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Master Card

Minakshee M. Basugade[1], Madhura M. Gaikwad[2], Ashwini B. Ghurake[3]

[1]*Department of Electronics & Telecommunication Engineering*

[2]*Bharati Vidyapeeth's college of Engineering, Kolhapur,(India)*

ABSTRACT

The idea behind this paper is to embed more than one bank account into single smart card so that the user can transact as he/she wishes with a single swipe. It provides the user one level higher convenience for accessing multiple accounts. Here the microcontroller acts like a smart card that holds the unique card number. In this proposed system admin module and user module are used. Admin module is responsible for entering the user details, user bank details, ATM card details. It is also responsible for clubbing of all accounts of an individual user and updating the database frequently. User module is the interactive module through which the user can log into the system and perform the transactions of the user's choice. Hereby, the users can access multiple accounts by entering a single PIN number.

Keywords: ATM cards, GSM, Multiple Account Access, OTP, RFID, Smart card, VSAT

1. INTRODUCTION

In this paper we are trying to reduce disadvantages of existing banking ATM (Automatic Teller Machine) system. In this proposed paper multiple banking accounts can be access by using single smart ATM card by following banking regulations and we can carry single ATM smart card for multiple bank accounts. In present ATMs, the customer identifies him or herself by inserting an ATM 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 personal Identification number (PIN) of four digits. The use of the password or PIN schemes was introduced in the early days of ATM machines and its use has continued into today's highly networked and distributed systems. The system does not further identify the user if the password or PIN is incorrectly entered because the password or PIN is meant to be known only to the authorized user. This allows anybody related or unrelated to the user who knows the user's password or PIN to make illegal access or withdrawal [2].

The main solution to this problem is OTP (One Time Password). Machine will generate OTP and send to user's registered mobile number. Then users have to type OTP and if it correct account will be open and user will be allowed for drawing money with his/her ATM card. Now the user can select the bank from which he/she is willing to perform transaction. After selecting the bank the request is sent to the corresponding bank through a network and links it with the banks server for accessing the database of the user or customer so that the transaction is processed [2].

1.1 Existing system

In existing ATM (Automated Teller Machine) 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 user swipes his ATM card at respective bank's ATM machine, then that ATM machine directly links to its bank server through VSAT to check whether the inserted card is valid or not. Transaction proceeds immediately if ATM card belongs to the same bank otherwise it connects to the respective banks server via NFS. Most of the modern ATMs make the use of magnetic strip card or a plastic card having an electromagnetic chip which carries the bank account information. The customer then verifies his or her identity by entering a pass code (i.e.) personal identification number (PIN) of four digits. As a security precaution most of the ATMs block the ATM card if the wrong PIN is entered several times (consequently 3 times), thus preventing an illegal or unauthorized access to the bank account. There is a limitation in transaction process; the customer who uses ATM card of some other bank account to withdraw money has to pay transaction fees if the withdrawal exceeds the transaction limit [2].

Disadvantages of Existing System

1. User has to carry separate card for each bank account and has to maintain the PIN for the each one
2. User has to pay extra charges when transactions are done from different bank's ATM other than ATM card after fee transactions over.
3. Absence of OTP (One Time Password) system technology [1].

1.2 Proposed System

The existing ATM implementation requires minor change in present banking network. The idea behind this embedded smart ATM card is that the customers can use a single ATM card to operate different bank accounts instead of having individual card for each bank account also to handle all the cards safely and maintain all the PINs secured is quite monotonous. The technology behind the product of the service is that adding all the user bank accounts to an embedded smart ATM card. In this the user swipes his/her smart card in the ATM machine, then it request for OTP (One Time Password) in the server side. Machine will generate OTP (One Time Password) and send to user's registered mobile number. Then user have to type OTP and if it correct account will be open and user will be allowed for drawing money with his/her ATM card, then it displays the list of all banks that the user is having account. Now the user can select the bank from which he/she is willing to perform transaction. After selecting the bank the request is sent to the corresponding bank through a network and links it with the banks server for accessing the database of the user or customer so that the transaction is processed [2].

Advantages of proposed system

1. User can perform transactions for all his bank accounts using single ATM card.
2. Enhanced security system.
3. It generates very time new password to customer registered mobile number.

4. More user friendly than present system.
5. Make banking system more inclusive [1].

2. FIGURES & TABLE

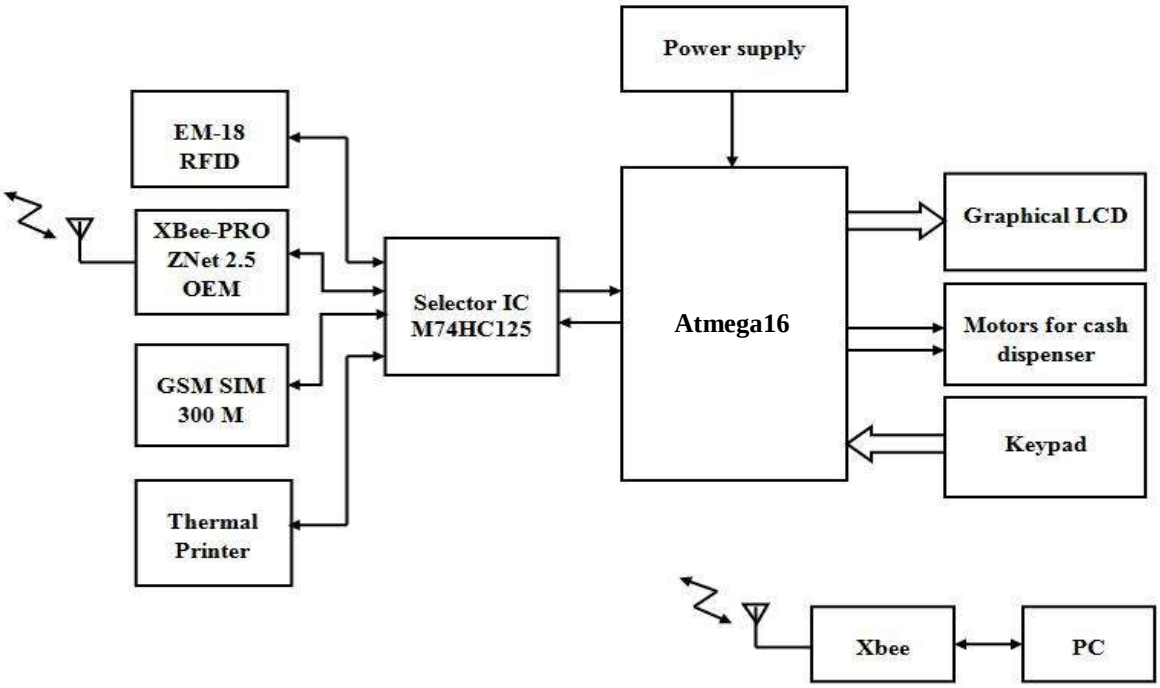

Fig1. Block diagram of proposed system

The circuit uses keypad and RFID as an input. When user waves the card in front of the RFID reader module, a serial code of the RFID card is sent to the UART of controller. The same information is send to the server's side through xbee end device. The serial code stored sent by RFID card is assigned to the particular user's information. ATM accesses this information by means of wireless communication that is xbee module. The OTP generated by a controller is sent by GSM slot installed at ATM to user's registered mobile number with the respective bank accounts. The sent OTP is temporarily stored in memory. When user enters the OTP, it is checked with the OTP stored in memory. If both OTPs match then the further process is initiated otherwise it asks to enter a correct OTP. After then it displays the list of the banks in which user has an account. User has to select the account from which he/she wishes to make withdrawal. After entering the withdrawal the transaction is processed and receipt is generated by thermal printer.

3. CONCLUSION

In present days, everyone has multiple bank accounts and has to maintain their passwords. In this single smart ATM card is implemented which provides easy access and also reduces the complexity so that the user can manage multiple bank accounts using single ATM card. For security purpose we have introduced concept of

OTP generation. The OTP generation is more viable method & provides sufficient security for ATM. The entire paper is based on embedded system technology so that the system becomes more reliable and safe.

REFERENCES

[1] Shivranjani S., Suganthi.I, Usha.V, Vinitha.M, Smitha Gayathri. D "Multiple Account Access using Single ATM Card" proceedings of 5th national conference on frontiers in communication & signal processing. Volume 6, special Issue 3, March 2017

[2] G. Manohar Babu, R. Anil Kumar, PG Scholar, "Multiple Banking System Accessing with Embedded Smart Card ATM by using ARM7 Based RFID & GSM Technology", Dept of Embedded Systems, Jyothishmathi College of Engineering and Technology, TS, India. Vol.07, Issue.08, July-2015, Pages:1319-1325