ISSN: 2321-2152

# IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152
www.ijmece .com
Vol 12 Issue1 Feb 2024

# DESIGNING OF SMART AND SECURE SINGLE ATM CARD FOR MULTIPLE BANK ACCOUNTS

**K KARTHIKA1, A. NANDHANA2, CH. MEGHANA3, A. ASHWINI4**

## ABSTRACT

This project's main objective is to integrate multiple bank accounts into one single smart card. Many bank charges ATM usage fees from the customers for different transactions. At present day, every customer has an individual ATM card for each and every bank in which he/she maintains account. So, while handling the cards, many passwords are involved. In order to overcome these difficulties, we embedded more than one bank account of the user in a single ATM smart card, therefore letting the user to swipe the card so that the respective individual can select the bank from which he/she is interested to carry out transaction.

## INTRODUCTION

Modern ATMs are implemented with high-security protection measures. They work under complex systems and networks to perform transactions. The data processed by ATM's are usually encrypted, but hackers can employ discreet hacking devices to hack accounts and withdraw the account's balance. Hence, to avoid such unauthorized transactions and to protect the confidentiality of the user, we raised the bars by introducing an additional security measure such as the biometrics. In the proposed method, the magnetic strip-based ATM card is replaced with RFID based card which have a unique number. The Arduino MEGA microcontroller is used to process the data from the sensor. The fingerprint module is used to authenticate the user. The user can register the bank details and also withdraw the amount from the registered bank details. Hence this system provides more secure and multiple bank account using single ATM card.

**ASSISTANT PROFESSOR1, UG SCHOLAR2,3&4**
**DEPARTMENT OF ECE, MALLA REDDY ENGINEERING COLLEGE FOR WOMEN, HYDERABAD**

## LITERATURE SURVEY

**Venka Reddy Maram, MirzaSajid Ali Baig, Narasappa Reddy "Advanced Security Management System for ATM's using GSM and MEMS",(IJI Tech) International Journal of innovative Technologies, ISSN 2321-8665 Vol.03,Issue.03, July-2015.**

"Design and Implementation of Multi-Application Smart Card for Banking and E-Payment System" by Oke A. O., Adeyemo S. A.,andOnibere S. A. (2013): This paper discusses the design and implementation of a multi-application smart card that can be used for banking and e- payment systems. The authors describe the architecture of the smart card, whichincludes multiple security features to protect against fraud and unauthorized access

[1]. "Smart Card Security: Threats, Risks andCountermeasures" by Abdul-Hameed A. O. and Jantan A. (2017): This paper provides an overview of smart card security threats and risks,and proposes a number of countermeasures to mitigate them. The authors highlight the importance of designing secure smart cardsystems, especially in the context of financialtransactions

[2]. "Multi-Bank ATM Card System" by S. Sivakumar and R. S. Thilagavathi (2011): This paper describes the design and implementation ofa multi-bank ATM card system that allows customers to access their accounts at multiplebanks using a single card. The authors discuss thechallenges of designing such a system, includingsecurity and interoperability issues

[3]. "A Secure Multi-Application Smart Card for Financial Transactions" by M. H. M. Arafa and H.El- Rewini (2011): This paper proposes a secure multiapplication smart card for financial transactions, which includes a number of security features to protect against various types of attacks.The authors evaluate the security of the proposed system using a number of metrics, and show that it provides strong protection against attacks .

The idea behind this project is to pull several bank accounts into a single smart card so that the user can do business as he wishes with a single tap. It provides more convenience for users to access multiple accounts. The device used is a PIC microcontroller. Here, the microcontroller acts like a smart card with a unique code. It is used in the system management module and user module of this contract. The management module is responsible for accessing user details, user company information, and ATM card details. It also monitors all accounts of club users and

updates information frequently. The user module is an interactive module where the user can enter the system and complete the action selected by the user. Therefore, users can access multiple accounts by entering a single passwordThe automated teller machine, or ATM, is a typeof electronic banking device that enables individuals to perform simple transactions without the help of a branch representative ATMS are commonly used by individuals with credit cards or debit cards to make quick cash withdrawals or deposit money. These convenientdevices allow people to perform various self-service transactions, such as transferring funds between accounts or paying for utilities. The first known instance of an ATM was shown in Londonin 1967. The use of ATMs quickly spread to all major nations on the earth. They are already in place in even the smallest island states like Kiribati and the Federated States of Micronesia. ATMs come in two main categories. Basic units simply let you obtain updated account balancesand cash withdrawals. The more sophisticatedmachines enable line of credit payments and transfers, receive deposits, and access account data. You frequently need to be a customer of the bank that runs the machine in order to utilize thecomplicated machines' advanced capabilities. This particular application's goal is to encourage users of different banks to utilize this solution to access their accounts and conduct transactions. They are not required to engage with several bank websites. The administrator can change the bank's current information and add new bank information. The admin will decide whether or not to accept a customer's registration to utilize this application. Customers should ask the Administrator for access to several bank accounts. He has access to account-related data.

**Aman Kumar, "Advance Security System for ATM", International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882 Volume 4, Issue 4, April 2015.**

The fundamental concept behind this project is to combine many bank accounts into a single smart card. In order to enable the user to swipe the card, we encoded multiple bank accounts of the user in a single ATM smart card. So that the appropriate person can choose the bank from which he or she is interested in doing a transaction. At present day, every customer has an individual ATM card for each and every bank in which he/she maintains various types of accounts. So, while handling the cards, many passwords

are involved. In order to overcome these difficulties, we embedded more than one bank account of the user in a single ATM smart card, therefore letting the user to swipe the card so that the respective individual can select the bank from which he/she is interested to carry out transaction.Even though modern ATMs are very secure and encrypted, thieves or hackers might try to find a way to crack the ATM's code and steal money. We created a single ATM card for multi banking in recent years to address the issue of individuals forgetting their password or misplacing their cards as time goes on. This allows us to successfully conduct transactions with our desired bank accounts from anywhere. We are using the Arduino UNO microcontroller, which is the finest for all such functions, to get around the problem of fraudulent transactions. Even in areas with poor service, the issue of password forgetfulness can be solved by employing a one-time password for a single ATM card using a Telegram bot.

**MoturiPhalgunaSatish, Bala Kishore. G , " Implementation of Bank Security System using GSM and Internet of Things", International Journal of Advanced Technology and Innovative Research, ISSN 2348–2370 Vol.09,Issue.09, August-2017.**

The Internet of Things (IoT) is one of the hottest topics in the technology sector, and with good reason. It influences the interaction of technological, economic, social, societal, and individual changes. Internet of things has been governing the electronics era with cloud services dominating the ever increasing electronics product segment. Security and safety has always become a basic necessity for urban population. The Implementation of the Bank Security System by Using GSM and IoT is developed into the security application. The main objective of this system is to develop an embedded system, which is used for ATM security applications. The embedded ATM authentication system is based on sensors & communication technology. In this paper when any disturbance takes place for the ATM machine then information is send through IoT and door is automatically closed then it will send the machine, by alerting the surrounding area using buzzer, at the same time total data will be uploaded in web page using IoT and puts alert message to consult person. In the same way if any fire occurred controller puts a message to consult person and uploads same data in web page using IoT. It also counts how many persons are entering into the ATM centre. This concept is not only a single ATM center; we can consider this ATM center as

node1 (like node1, node2, node3……. Etc) are connected to web page through IoT module (ESP 8266). So that if there is any disturbance or any fire accident in any node we can get the area information through IoT to the web page along with buzzerThe Internet of Things (IoT) is the physical network of things or objects devices, buildings, vehicles, and other items embedded with electronics, software, sensors, and network connectivity that enables these things or objects to collect and exchange data. An anti-theft system is any device or method used to prevent or deter the unauthorized appropriation of items considered valuable. Theft prevention based on IOT provides a system. Internet of Things is expected to produce high degree of human to machine communication along with machine to machine communication. This project proposes the security system using IOT, which prevents theft in home, bank etc. The primary objective of this project is to reduce human workAutomation has always been a prime factor for security system. We aimed in the project is to design and implement a security system. System that offers controllability through a hand held mobile phone by means of IOT. As we know that over the past three decades, consumers have been largely depending on and trust Automatic Teller Machine, known as ATM machine to conveniently meet there banking needs. Using an ATM, customers can access their bank accounts in order to make cash withdrawals, debit card cash advances, and check their account balances as well as purchase prepaid cell phone credit. Most ATMs are connected to interbank networks, enabling people to withdraw and deposit money from machines not belonging to bank where they have their accounts or in the countries where their account are held. Despite the numerous advantages of AT M system, ATM fraud has recently become more widespread. Fraud technique such as card skimming, shoulders surfing etc have been observed recently. In order to increase the level of security of the ATM networks use of biometric technique for verification along with existing PIN has been thought of a solution to decrease the increasing number of frauds. Also in rural areas people are not educated enough to use the ATM machines so, use of only biometric verification can help those people access the ATMs in an easier manner and hence increase its popularity among rural masses. A WSN (wireless sensor network) generally consists of base station (or) gateway that can communicate with a number of wireless sensors via a radio link. Power unit produces the power. Data

Processing unit have the micro- controller, which is the fully responsible to get sensed data and transmit over the network microcontroller performs tasks, processes data and controls the functionality of other components in the sensor node. Sensing unit has the sensors and analog to digital converter (ADC) to convert analog sensed signal to digital signal. The ideal WSN is networked and scalable, consumes very little power, is smart and software programmable, capable of fast data acquisition ,reliable and accurate over the long term, costs little to purchase and install, and requires no real maintenance. Selecting the optimum sensors and wireless communication slink requires knowledge of the application and problem definition.

**Arpita V Naik, NehaNanaiah N, Sheral Paul, Soniya R Naik, Geethalaxmi "Unification of Multiple Account using Single ATM Card", International Journal of Scientific Research and Review ISSN No.: 2279-543X Volume 07, Issue 05, May 2019.**

The reader, keypad, camera, PC and display device connected to a microcontroller. We are using RFID smart card as ATM Card for transaction. User can create account and get the ATM card from the bank. User can integrate all his accounts in which user is having access to bank can be integrated in this single ATM card with specific PIN numbers accordingly. User face is also recognized for the verification part. User behaviour is monitored through HMM (Hidden Markov Model) Model. User can include all his family members' accounts details also in the same card. Four digits PIN number can be entered through Keypad. If the entered PIN number is correct, then camera is automatically on and captures the face of the user and vein sensor is used for verification. After authentication process user can withdraw amount from atm. Server will monitor the user's frequency of amount (average amount withdrawal) and number of transaction count (normally three transaction times at a time) using HMM model. If any variation is detected during transaction, it will ask to enter security number/formula, which is set by the user at the time of registration. Now the transaction is possible only, when the customer will enter the correct code / formula. In [2] The proposed systemprovides Integration of Big Data, Business analytical and RFID technology which are recent trends in IT, which is a challengeoriented activity. We have modified andimplemented this application for developing Banking sector particularly for

Debit / ATM \card section. We can use RFID smart card as ATM Card for transaction. User can create account and get the ATM card from the bank. The user can integrate all his bank accounts which can be integrated in this single card with unique PIN numbers accordingly. User behaviour is monitored through HMM Model and he can set up a formula-based authentication. The user can include all his family members' accounts details to this same card. The user can withdraw cash from their accounts after successful authentication of the corresponding PIN numbers. In [3] the proposed system embeds 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. The hardware used is PIC microcontroller. 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. 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. In this the user swipes his/her smart card in the ATMmachine, then it requests for OTP in the server side. 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 so that the transaction is processed. In [4] the system proposes Multi Account Embedded ATM card. To provide security we introduced fingerprint-based authentication. It reduces the cost of inter-banking transactions as interfacing different bank databases is a resource consuming thing. The technology behind the product of the service is that adding all the user bank accounts to a multi account ATM card. In order to provide the access for the customer to all his/her bank account, first the fingerprint-based authentication of the customer needs to be done. By introducing the biometric analysis (fingerprint authentication) we provide high security for the customer because it is very difficult to fake. The fingerprint reader captures the fingerprint image and extracts the unique

features of the fingerprint called template. This template is stored in system data base. When the authentication is to be performed, at that time the fingerprint reader reads the fingerprint of the user and extracts the unique features and this is compared with the previously stored template, which is in system data base. In [5] the proposed system in which the embedded system is developed based on ARM7(LPC 2148) microcontroller, whenever the person puts his smartcard on the reader the system will detect the authorized persons then it asks for pin and sendsthe message to the person with his registered mobile number using GSM technology. The GSM module interfaced to the ARM7 microcontroller and the pin is entered by using keypad. 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 requests 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 is 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. In [6] the proposed system aims at improvising the security and authenticity of the Automated Teller Machine (ATM) using a trusted third-party application. This system would in turn benefit all the customers who have a valid ATM card registered officially with their mobile number. This system provides the following facilities of withdrawing currency at any remote terminal, verification of the end users identity using Personal Identification Number and an authentic One-TimePasskey (Pk) validation through the mobile. The customers, without any insider privileges, can withdraw currency without being detected by anymechanisms of theft of card and eaves dropping of the Password from the card holders within the terminal software are also the major threat yet to be addressed. A basic solution is the ATM systems having a two-tier authentication Pk and Random Security Question (RSQ) are being generated and validated from the user's input from the ATM Terminal with authenticity being ensured and the confidentiality being maintained. In such a

system, the correctness burden on the terminal's code is significantly less as the customers have been given the chance to authorize themselves from their handheld devices and are allowed to withdraw currency in terminal only after their identity is proved by a series of authentication procedures. In this paper along with the dual tier authentication implementation, the issues arise along with them and the solvencies to these issues related to the generation of the RSQ and Pk independent and unique for each session are addressed.

**Existing system**

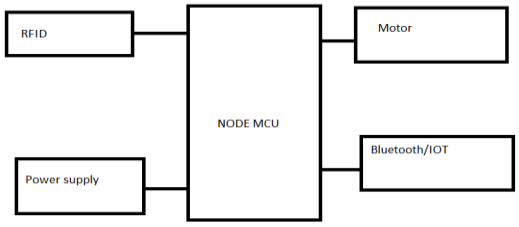
Implement a fingerprint sensor on the card for biometric authentication, ensuring that only the authorized cardholder can access the accounts. NFC (Near Field Communication): Enable contactless payments for enhanced convenience. Users can simply tap their card on compatible terminals for quick transactions. Use a secure microcontroller or chip that complies with international standards (e.g., EMV) to store and process sensitive data securely. Develop a mobile app that syncs with the card, allowing users to manage multiple bank accounts associated with the card, set transaction limits, and receive real-time notifications. eCVV (Dynamic Card Verification Value): Implement a dynamic CVV that changes periodically, adding an extra layer of security to online transactions. Consider integrating blockchain to enhance the security and transparency of transactions. This can also help prevent fraud and unauthorized access. Biometric Confirmation for High-Value For high-value transactions, require additional biometric confirmation through the fingerprint sensor. SMS or App-Based Authentication: Implement 2FA for additional security. Users receive a one-time code via SMS or a dedicated authentication app to complete transactions. End-to-End Encryption: Ensure that all communication between the card, ATM, and mobile app is encrypted to prevent data interception. Allow users to freeze and unfreeze their cards through the mobile app in case the card is lost or stolen.Implement behavioral analytics to detect unusual spending patterns and flag potential fraudulent activities, triggering alerts for both the user and the bank. OTA (Over-The-Air) Updates: Provide a mechanism for over-the-air updates to ensure that the card's software and security features are up-to-date. Security Awareness Campaigns: Educate users about safe practices, such as not sharing PINs or leaving the card unattended. Compliance with Data Protection Ensure compliance with relevant

data protection and privacy laws to protect user information. Instant Customer Support: Provide a dedicated helpline for users to report issues or concerns immediately.

**Proposed system**

In the proposed method, the magnetic strip-based ATM card is replaced with RFID based card which have a unique number. The Arduino MEGA microcontroller is used to process the data from the sensor. The user can register the bank details and also withdraw the amount from the registered bank details. Hence this system provides more secure and multiple bank account using single ATM card. A power supply of +5V is given to the circuit as an input. Arduino mega acts as a microcontroller that simultaneously stores data given to it. The ATM card consist of a magnetic strip containing a unique 12-digit number which acts as an RFID tag. This tag is read by a passive RFID reader (here EM-18 module) which is connected to the microcontroller through serial communication (UART). A 4x4 keypad is connected to the microcontroller that acts as an input to enter the 4-digit pin. Once the authenticity of the pin is confirmed the finger print of the user is verified using an optical fingerprint reader. The money is deposited or withdrew through servo motor that rotates 180 degree if the finger print matches the biometric data. On the other hand, if the finger print does not match, the buzzer starts ringing. Finally, irrespective of success or failure of the transaction a message or call is sent to the user through GSM module (SIM800L) which is 2G based network that uses AT commands.

**BLOCK DIAGRAM**




**CONCLUSION**

In this project, the user can manage his/her multiple accounts in various banks with the help of this single smart card ATM which provides easy access and reduces the complexity of managing more than one ATM card and their respective passwords. Here we provided the user with biometrics in order to create a viable method of identifying user's sufficient security level for the ATM system. The security features were enhanced largely for the stability and reliability of the owner's recognition. The whole system is built on the technology of embedded system which makes the system safe, reliable and easy to

implement. Hence the vulnerabilities of the ATM fraud are reduced.

**REFERENCES**

[1] Venka Reddy Maram, MirzaSajid Ali Baig, Narasappa Reddy "Advanced Security Management System for ATM's using GSM and MEMS",(IJI Tech) International Journal of innovative Technologies, ISSN 2321-8665 Vol.03,Issue.03, July-2015.

[2] Aman Kumar, "Advance Security System for ATM", International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882 Volume 4, Issue 4, April 2015.

[3] MoturiPhalgunaSatish, Bala Kishore. G , " Implementation of Bank Security System using GSM and Internet of Things", International Journal of Advanced Technology and Innovative Research, ISSN 2348–2370 Vol.09,Issue.09, August-2017.

[4] Shinde S.P, Chingale R.R., Dhane D.C., Vader P.B, "International Research Journal of Engineering and Technology (IRJEFT)", e-ISSN: 2395 -0056, p-ISSN: 2395-0072, Volume: 04 Issue:03, Mar -2017.

[5] SudhakarHallur, ManjunathBajantri, SagarSantaji, "International Research Journal of Engineering and Technology (IRJEFT)", e-ISSN:2395-0056, p-ISSN: 2395-0072, Volume:05, Issue:06, June-2018.

[6] K.Sridharan ,K.G.YuvaraajK.C.RahulS.TamilKanalS.D. Ashok Kumar , " Multi Bank ATM Family Card: Integration Of Multi Bank Multiple User In Single Card With User Behavior Monitoring Using HMM & Formula Verification" , International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 , p-ISSN: 2395-0072 ,Volume: 04 Issue: 03 , Mar -2017.

[7] B. Saranya, N. Sri Priyadarshini, R. Suvetha, K. Uma Bharathy, "ATM Security System Using Arduino", International Conference On Advanced Computing and Communication Systems (ICACCS),2020.

[8] Pavan S. Rane, Prashant P. Sawat, Sourabh B. Shinde, Nitin A. Dawande, "ATM Security", International Journal of Advance Engineering and Research Development, Volume 5, Issue 06, June -2018.

[9] Christiawan, BayuAjiSahar, Azel Fayyad Rahardian, ElvayandriMuchtar, "Fingershield ATM – ATM Security System using Fingerprint Authentication", Bandung Institute of Technology, Bandung 40132, Indonesia ,2019.

[10] Arpita V Naik, NehaNanaiah N, Sheral Paul, Soniya R Naik, Geethalaxmi "Unification of Multiple Account using Single ATM Card", International Journal of Scientific Research and Review ISSN No.: 2279-543X Volume 07, Issue 05, May 2019.