Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 06, June -2018

ATM SECURITY

[1]Pavan S. Rane, [2]Prashant P. Sawat, [3]Sourabh B. Shinde, [4]Prof. Nitin A. Dawande

Department of Electronics and Telecommunication Engineering
Dr. D Y PATIL COLLEGE OF ENGINEERING, AMBI, PUNE

Abstract — *Security is a major issue in Automated Teller Machine (ATM).with the wide spread utilization of electronic transactions it is necessary to increase customers recognition accuracy. Biometric systems can offer convenient and secure mode of authentication to the customers.*

Nowadays banking sector is one of the most important parts of a human day to day life. Banking facilities are widely used by people for their economies activities. Automatic Teller Machine (ATM) is an electronic machine which is used for accessing a bank account from anywhere without the help of bank staff. The user can perform several banking activities like cash withdrawal, money transfer with the help of ATM. It is observed that the numbers of crime related to ATM increased hence need to provide better security to ATM machine. There are different technologies which are used to provide security to ATM machine which include – Biometric technology, RFID technology etc. Biometric technology includes fingerprint and face recognition system. In this paper survey of different technologies for ATM security is presented. In these technologies, there are some limitations. By comparing various technologies which are used for ATM security it observes that fingerprint technology appears better and more secure than other technologies.

In this project we used matlab for face recognition. 1st stage is face recognition. if face recognition done or successfully than rfid activated. If rfid read right string than they can get atm access otherwise buzzer will on.

Keywords- *ARM 11,DC MOTOR ,BUZZER,RFID READER, CAMERA.*

I. INTRODUCTION

The full form of ATM is Automated Teller Machine. It is an electronic telecommunications device that enables the customers of a financial institution to perform financial transactions, particularly cash withdrawal, without the need for a human cashier, clerk or bank teller [1]. ATMIA is the ATM Industry Association, which has a record that close to 3 million ATMs are currently installed worldwide. Along with the growing convenience and feasibility of the ATMs, there is also an increase in the amount of ATM thefts and frauds, which are developing at an alarming rate. In the war of functionality versus security, the functionality wins more often. Security has always been viewed upon as an overhead or afterthought by software developers. But in the case of banking and money transactions, the security should hold highest priority. Increase in daily attacks on ATM and banking security [1] the developers getting on right track and putting security their important aspect in developing projects.

The multifactor authentication is an approach to authentication which requires the presentation of two or more authentication factors: a knowledge factor ("something only the user knows"), a possession factor ("something only the user has"), and an inherence factor ("something only the user is"). After presentation, each factor must be validated by the other party for authentication to occur [2]. In present days the ATM holds only one thing (i.e. PIN) to secure the money saved in the bank if we are not considering the physical attacks. In our system we are going beyond this level of security to enhance security of the ATM. We introduce the concept of one time password (OTP) [3] in ATM banking. Our system will provide the second level of security using different factors to generate OTP. This will send over customer's mobile number stored in records.

In secure ATM, user will have to register mobile and its IMEI number in bank system. When user puts/swipes card into machine, user get request to insert PIN (which is current way of ATM banking). In the proposed system user will get OTP on mobile. When user enters OTP to the system, he/she will be having access to the machine else no transaction can be made.

II. LITERATURE SURVEY

We have gone through the different types of researched work and papers on ATM security system some of them and have been reported in the literature. However, few relevant and significant works are reviewed here.Crime at ATMs has become a nationwide issue that faces not only customers, but also bank operators and this financial crime case rises repeatedly in recent years. A lot of criminals tamper with the ATM terminal and steal customers' card details by illegal means. Once users' bank card is lost and the password is stolen, the users' account is vulnerable to attack.

Traditional ATM systems authenticate generally by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects. The prevailing techniques of user authentication, which involves the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations. Passwords and PINs can be illicitly acquired by direct covert observation.

When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords - birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be. Biometric authentication technology may solve this problem since a person's biometric data is undeniably connected to its owner, is nontransferable and unique for every individual.[3]

The system can compare scans to records stored in a central or local database or even on a smart card. Biometrics can be defined as a measurable physiological and behavioral characteristic that can be captured and subsequently compared with another instance at the time of verification.

It is automated methods of recognizing a person based on a physiological or behavioral characteristic. It is a measure of an individual's unique physical or behavioral characteristics to recognize or authenticate its identity.

Common physical biometrics characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioral characteristics are signature and voice. Biometrics technologies are a secure means of authentication because biometrics data are unique, cannot be shared, cannot be copied and cannot be lost.

Author Jaydeep Shamdasani et al Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 4, Issue 4(Version 5), April 2014, pp.74-78 [1] have established a system which is based on ARM architecture.

Securing ATM with OTP and Biometric Mohammed Hamid Khan Shah and Anchor Kutchhi Engineering College Mumbai, India. Email: mailathamid@gmail.comThis project is also considering application based problem of ATM where the factors like, user forgot the mobile device at home, mobile battery is down, and user is not in the network coverage to make difficulties in OTP security service.

For covering such difficulties another option is given in the ATM that is Biometric. By using biometric authentication legitimate user can do transaction even if he/she is not having his/her mobile device for receiving OTP.[2]

The proposed ATM client authentication system depends on fingerprint recognition which is developed after analyzing existing ATM systems. The ARM 9 microcontroller (Friendly ARM) is used as the brain of these embedded systems along with fingerprint recognition module and GSM Module.[3]

III. System architecture

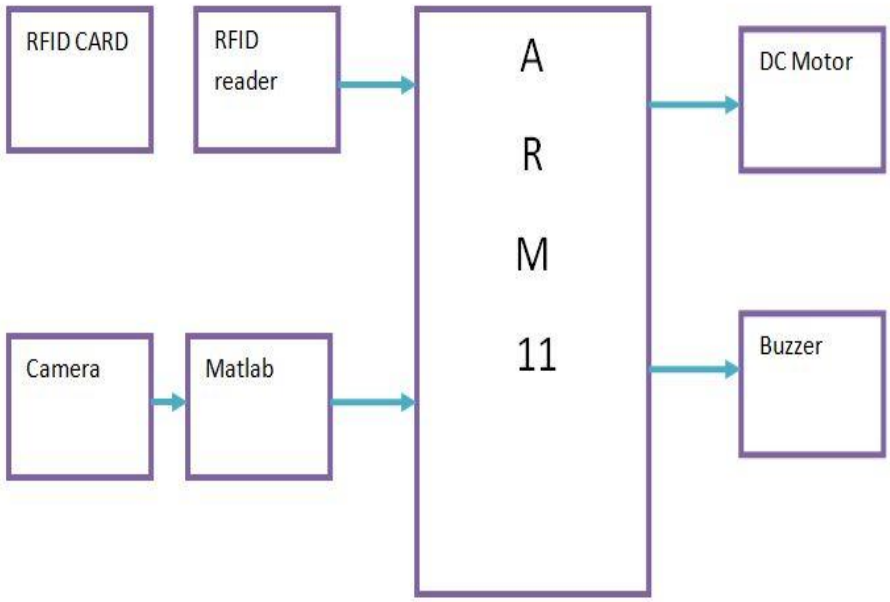
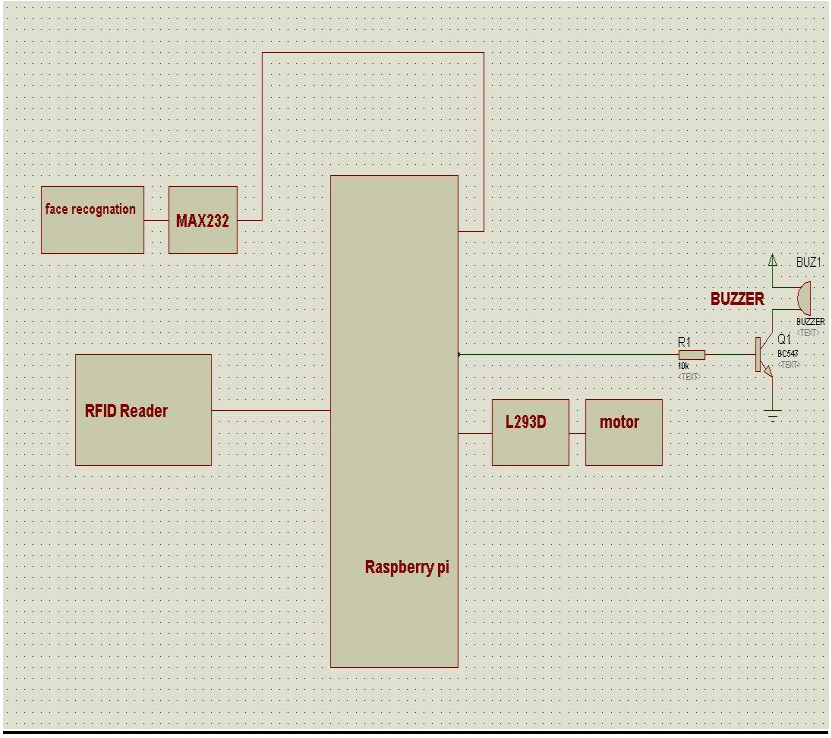


Figure: System Architecture

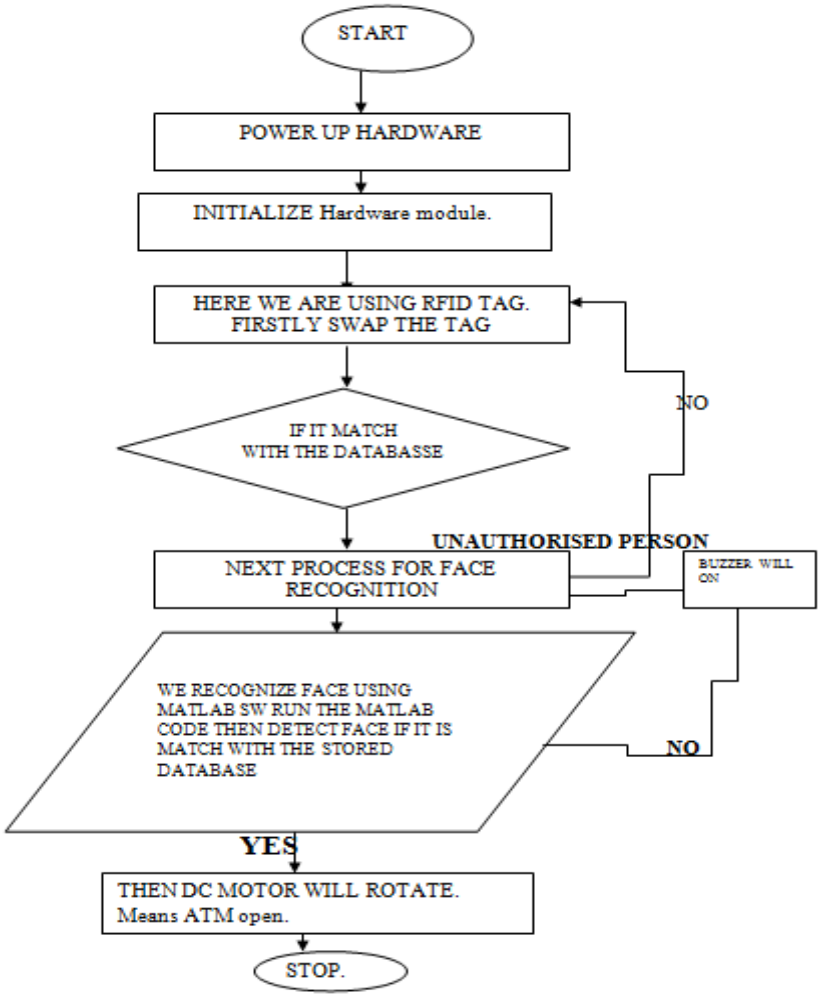
IV. Proposed System

- The process of ATM transaction starts when face recognized. MATLAB IDE used for face recognition purpose, then next step is rfid card, unique for each person, to the RFID reader for scanning. The account related to the unique RFID number will access. When this step match with stored rfid number than the transaction will be allowed. Otherwise, the account information will not be displayed and further activity will be disabled.

V. Circuit Diagram



VI. FLOW CHART



VII. ADVANTAGES

- This project implementation is used for securing purpose to amount.nothing but anti thefting.
- Protecting to our banking
- saves money.
- Freedomful from our fear about security.

VIII. Goals and Objectives

The aim of our project to reduce the amount thef & hacking through ATMs.
Now a days there is no secure for money.
Talking about ATM security, Personal identification number (PIN) or password is very important.
PIN or password is widely used to secure financial/confidential information of customers from unauthorized access.
An ATM is a IT enabled Electro-mechanical system that has connectivity to the accounts of a banking system.

VI. CONCLUSION

Face recognition is a very useful and versatile technique. IT is highly accurate technique. This technique has successful applications. This technique increases both privacy and identity.
The growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, banks accounts and computer systems often use PIN's for identification and security clearances. Conventional method of identification based on possession of ID cards or exclusive knowledge like a social security number or a password are not all together reliable. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords birthdays, phone numbers and social security numbers. This paper may solve this problem and useful for detecting a fraud .
It is used in Bank sector and any ATM related security. It is also called as thief tracking system. As there is a scope for improvement and as a future implementation we can add a tracking chip on ATM card for tracing the location of card which will help in providing users assistance.
Face recognition technique finds a wide range of applications in fields involving high security. It is advancement in the field of technology thereby giving a great push to the technology industry. Many projects related to security and control can be implemented by this face recognition technique.

REFERENCES

[1] *ARM7 Based Smart ATM Access & Security System Using Fingerprint Recognition & GSM Technology Khatmode Ranjit P1 , Kulkarni Ramchandra V2 , Ghodke Bharat S3 , Prof. P. P. Chitte4 , Prof. Anap S. D 5 1 Student of B.E. Electronics, Pravara Rural engineering college, loni, Maharashtra,*

[2] *Atm Client Authentication System Using Biometric Identifier & Otp Jaydeep Shamdasani*1, Prof .P.N.Matte*2 , *1(E &TC department, GHRCEM Pune, India.) *2(Head of E&TC Department, GHRCEM Pune, India)*

[3] *IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 20, NO. 8, AUGUST 1998 Fingerprint Image Enhancement: Algorithm and Performance Evaluation by Lin Hong, Student Member, IEEE, Yifei Wan, and Anil Jain, Fellow, IEEE.*

[4] *International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X Implementation of ATM Security by Using Fingerprint recognition and GSM by PENNAM KRISHNAMURTHY & MR. M. MADDHUSUDHAN REDDDY*

[5] *An Improved Method for Extraction of Fingerprint Features Jianwei Yang, Lifeng Liu, and Tianzi Jiang*, Member, IEEE National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Beijing 100080, P. R. China.*

[6] *Volume 3, No. 11, November 2012 Journal of Global Research in Computer Science RESEARCH PAPER HIGH PROTECTION HUMAN IRIS AUTHENTICATION IN NEW ATM TERMINAL DESIGN USING BIOMETRICS MECHANISM.*

[7] *Indian Journal of Science and Technology Supplementary Article ATM Terminal Design using Biological Technology by V. Khanaa and Krishna Mohanta.*

