International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Modernizing ATM Security with Biometrics by Using LabVIEW

K. Rambabu[1], M. Ratnakar Reddy[2], V. Pavan Kumar[3], S. Naveen Kumar[4]
[1]*Dept. of Electronics and communication, BVRIT, Telangana*

Abstract: ***In today's world the usage of currencies is moving towards virtual money. One of the at most important things that helped in making the transition towards virtual cash has been Automated Teller Machine (ATM). In order to give a better security here is a proposed system which would be helpful in enhancing the machines security. In this proposed system we enhanced security issue by implementing biometric based finger print where an unauthenticated entry would lead to a message and a mail forwarded to card owner with no delay.***
Keywords: ***Automated Teller Machine, LabVIEW, Arduino, Biometric.***

I. INTRODUCTION

ATM is Automated Teller Machine. Now it's making peoples life very easy as they get their money when they need. So, they do not need to carry either big amount of money or the cheque book all the time. To get rid from this burden they need to deposit money in the bank by opening an account and then the bank will be given a Card i.e. an ATM card with a PIN number to them. By using that they can withdraw money from any ATM machine of that bank. When they insert the card in the machine and the PIN number the machine will show few instructions on the screen [3]. By that time verification (PIN Number and Account Number) will be done with the main bank computer as they are connected. If the verification is correct then the user will choose an instruction and the ATM will dispense money to the card holder. In the consideration of ATM, the issue of security is of paramount importance because all over the world, there is an increasing use of ATMs and so the risks of hacking turn to be a reality more than ever before. In the past, the function of ATMs was to deliver cash in the form of bank notes and to debit a corresponding bank account. Cards were used to identify the user. As for the withdrawal of money, different methods were used. For instance, punched cards were used. By the use of such cards, only one payment was authorized. Thereby, a user had to get a supply of cards from his/her bank because the punched cards were not returned to the user. Another example was the use of a magnetic card which had a limited life. The use of such cards allowed; for instance, twenty withdrawals of money [1][4]. From the beginning, personal identification number (PIN) has been of very great importance in the overall operation. The use of it has been done with the aim to decrease the risks that might result from the loss of cards and the misuses that might be connected to that. In fact, in the past as well as in the present, there have been different aspects in the consideration of the designing and the communicative basics of Automated Teller Machines. One aspect of it has been how communication between its participants could be possible.[2][4] The second of it has been to take into consideration the purposes which could be a part and a parcel of any communicative act. In this context, there are different participants involved in ATMs communication. To cite but a few of them, in an ATM communication, there are remote partners and interfaces to the outside world and these interfaces are in their turn subject to more than one classification. The first interface represents the relationship between the End-user and Automated Teller Machine. The second interface occurs between the ATM and the central bank computer.

II. PROPOSED SCHEME

In the proposed system, the security of ATM is to increase to a new level. In order to do that in this project PIN number has been replaced with biometric fingerprint scanner. Biometrics-based authentication offers several advantages over other authentication. Fingerprint technology in particular, can provide a much more accurate and reliable user authentication method. Biometrics is a rapidly advancing field that is concerned with identifying a person based on his or physiological or behavioral characteristics. As the Automated Teller Machines (ATM) technology is advancing, fraudsters are devising different skills to beat the security of ATM operations. Various forms of fraud are perpetuated, ranging from: ATM card theft, skimming, pin theft, card reader techniques, pin pad techniques, force withdrawals and lot more. Managing the risk associated with ATM fraud as well as diminishing its impact is an important issue that faces financial institutions as fraud techniques have become more advanced with increased occurrences.
Considering the numerous security challenges encountered by Automated Teller Machines (ATM) and users and given that the existing security in the ATM system has not been able to address these challenges, there is the need to enhance the ATM security system to overcome these challenges. This project focuses on how to enhance security of transactions in ATM system using

fingerprint. The aim of this project therefore is to develop ATM simulator based fingerprint verification operations in order to reduce frauds associated with the use of ATM and keep the customer and the law enforcement agencies of unauthorized assessors. In addition to fingerprint the proposed project also send SMS alerts to registered mobile number using GSM module. When an unauthorized person tries to access the account a signal through microcontroller reaches to LabVIEW display after that the camera captures the image and sends it to the registered Email ID.

III. DESIGN ANALYSIS

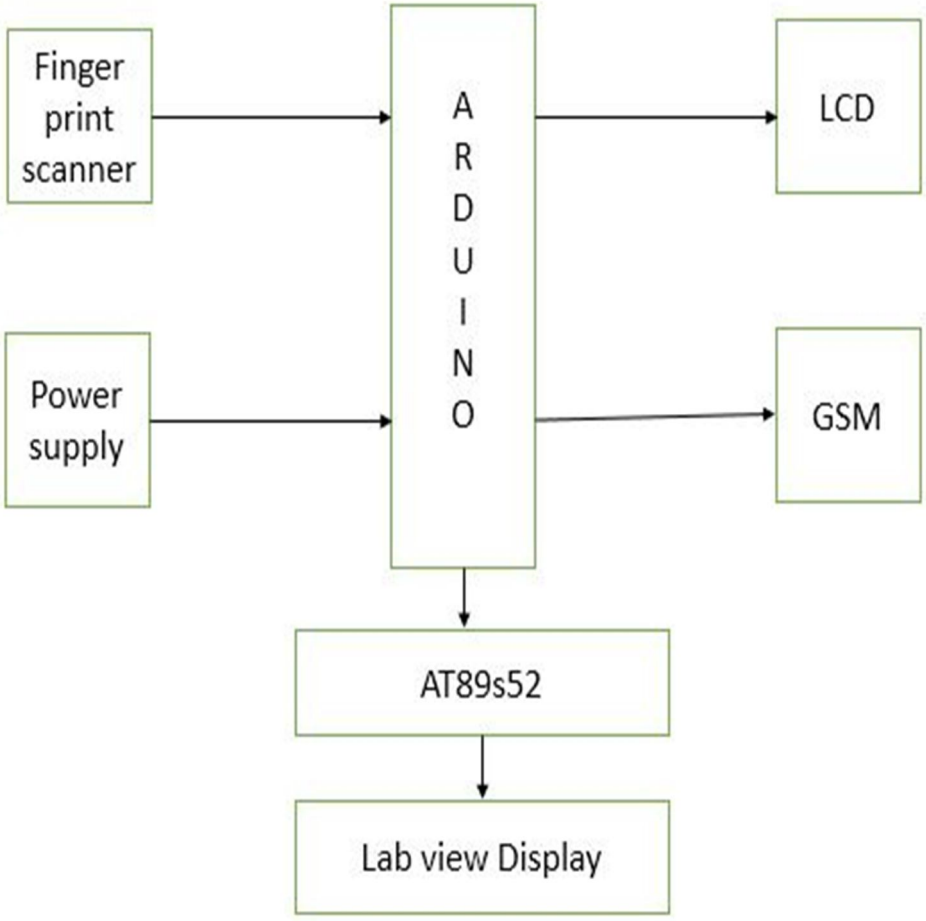

Fig 1 Block diagram of proposed system

A. Finger Print Scanner

Finger print scanner features includes: easy restructure, powerful functions, compatible with PC and multiple-functions in one module: Fingerprint enrollment, image process, characters acquisition, fingerprint template creation, fingerprint template storage, fingerprint compare (1: 1, 1: N), fingerprint delete. This module can work with different devices based on UAWRT such as PC, SCM and so on. Only easy circuits and fingerprint module can enhance your product into fingerprint authentication power. It is widely used by electronics business, information security, access control, identity authentication and other security industry.

B. LabVIEW

LabVIEW (short for Laboratory Virtual Instrumentation Engineering Workbench) is a platform and development environment for a visual programming language from National Instruments. The graphical language is named "G". Originally released for the Apple Macintosh in 1986, LabVIEW is commonly used for data acquisition, instrument control, and industrial automation.

Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

IV. FLOW CHART

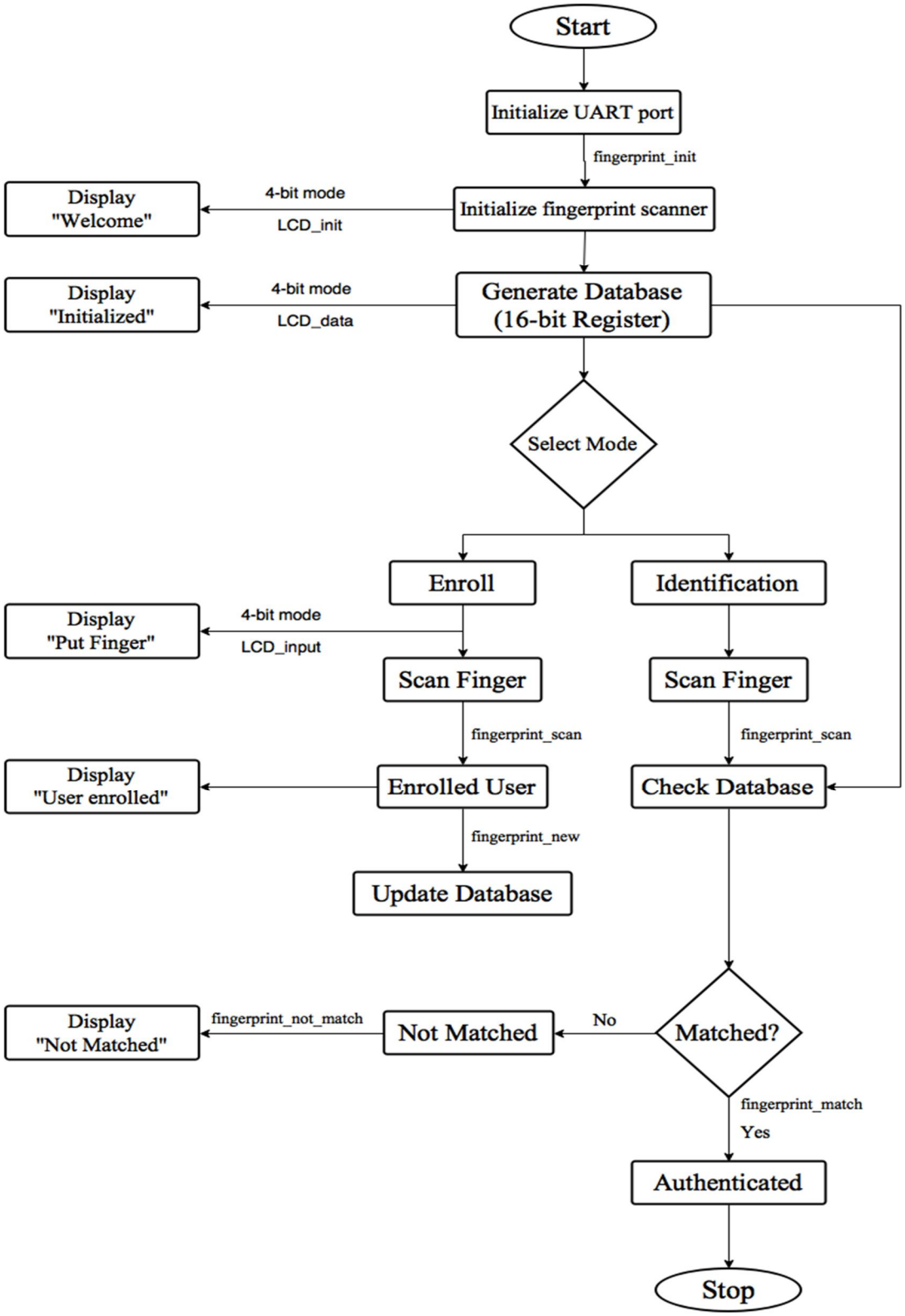

Fig 2 Flow chart of proposed system

V. RESULTS

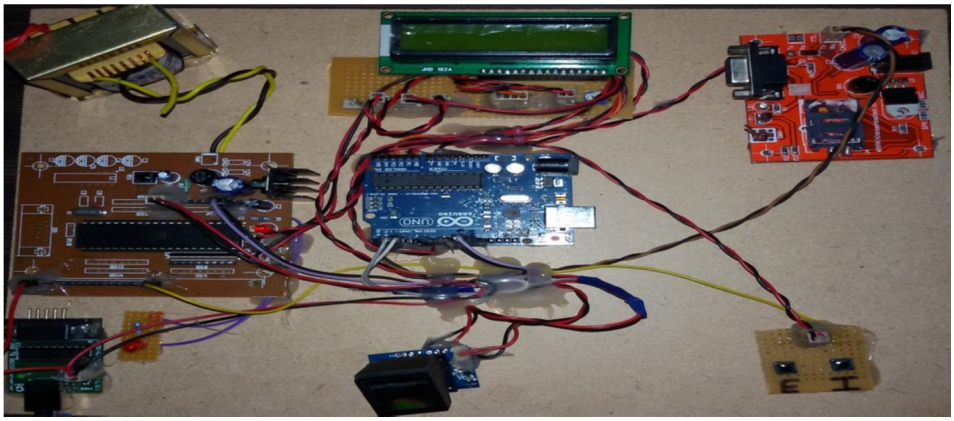

Fig 3 designed hardware

VI. CONCLUSION

The main reason for introducing biometric systems is to increase overall security. Biometrics offers greater security and convenience than traditional methods of personal recognition. In some applications, biometrics can replace or supplement the existing technology. In others, it is the only viable approach. Decision-makers need to understand the level of security guaranteed through the use of biometric systems and the difference that can exist between the perception and the reality of the sense of security provided. The biometric system is only one part of an overall identification or authentication process, and the other parts of that process will play an equal role in determining its effectiveness.

REFERENCES

[1] G. R. Jebaline and S. Gomathi, "A novel method to enhance the security of ATM using biometrics," Circuit, Power and Computing Technologies (ICCPCT), 2015 International Conference on, Nagercoil, 2015, pp. 1-4.
[2] S. Ray, S. Das and A. Sen, "An intelligent vision system for monitoring security and surveillance of ATM," 2015 Annual IEEE India Conference (INDICON), New Delhi, India, 2015, pp. 1-5.
[3] Jain, A.K.; Ross, A.; Prabhakar, S., "An introduction to biometric recognition," Circuits and Systems for Video Technology, IEEE Transactions on, Vol. 14, no. 1, pp. 4,20, Jan. 2004 doi: 10.1109/TCSVT.2003.818349
[4] Patiyoot, D.; Shepherd, S.J., "Security issues for wireless ATM network," Universal Personal Communications, 1998. ICUP'98. IEEE 1998 International Conference on, vol.2, no., 5-9 Oct 1998 doi: 10.1109/ICUPC.1998.733713