GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

ATM SECURITY IMPROVEMENT USING FINGER PRINT

Neelam Verma[1], Rakesh Patel[2], Priya Bag[3]
Student,B.E.(IT) Kirodimal Institute of Technology,Raigarh(C.G.),India[1,3]
Lecturer,Department of Information Technology Kirodimal Institute of Technology Raigarh(C.G.),India[2]

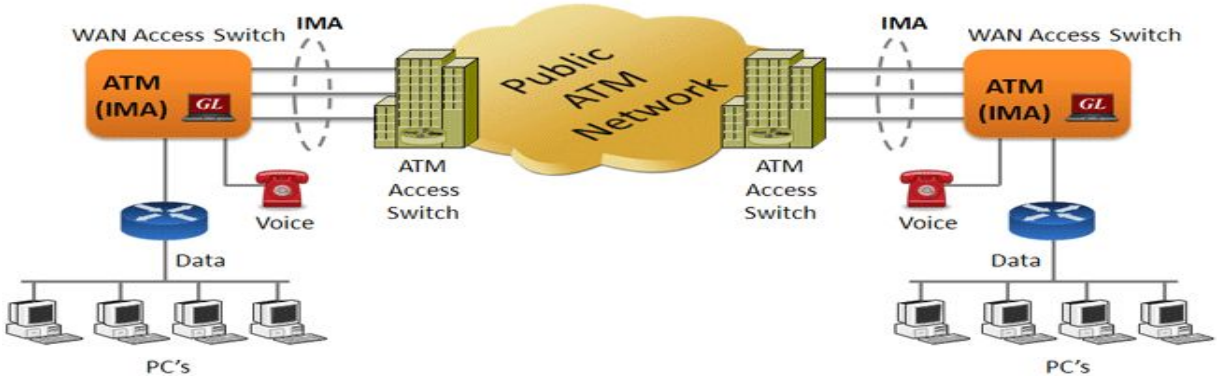
ABSTRACT

The growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication We provide the first published estimates of the difficulty of guessing a human-chosen 4- digit PIN. We begin with two large sets of 4-digit sequences chosen outside banking for online passwords and smartphone unlock-codes. In this paper the existing security of the ATM (Automated Teller Machine) system has been improved by integrating the fingerprint of the user into the bank's database as to further authenticate it. In this scheme, a fingerprint biometric technique is fused with the ATM for person authentication to ameliorate the security level. Then change the security level of next generation.

Keyword - ATM ,PIN ,FINGERPRINT, BIOMATRICS,SECURITY

I. INTRODUCTION

Since the introduction of the first automated teller machine (ATM) in 1967, perpetrators have been devising ways to try to steal the cash inside. Because ATMs eliminate the need for round-the clock human involvement and tend to be located in places that make them more vulnerable to attack, they are often attractive targets for perpetrators.ATM crime is not limited to the theft of cash in the ATM. Many ATM attacks seek to obtain a consumer's personal information, such as their card number and personal identification number (PIN). Personal identification number (PIN) or password is one important aspect in ATM security system .This study focuses on how to enhance security of transactions in ATM system using fingerprint. The aim of this study therefore is to develop ATM simulator based fingerprint verification operations in order to reduce frauds associated with the use of ATM.

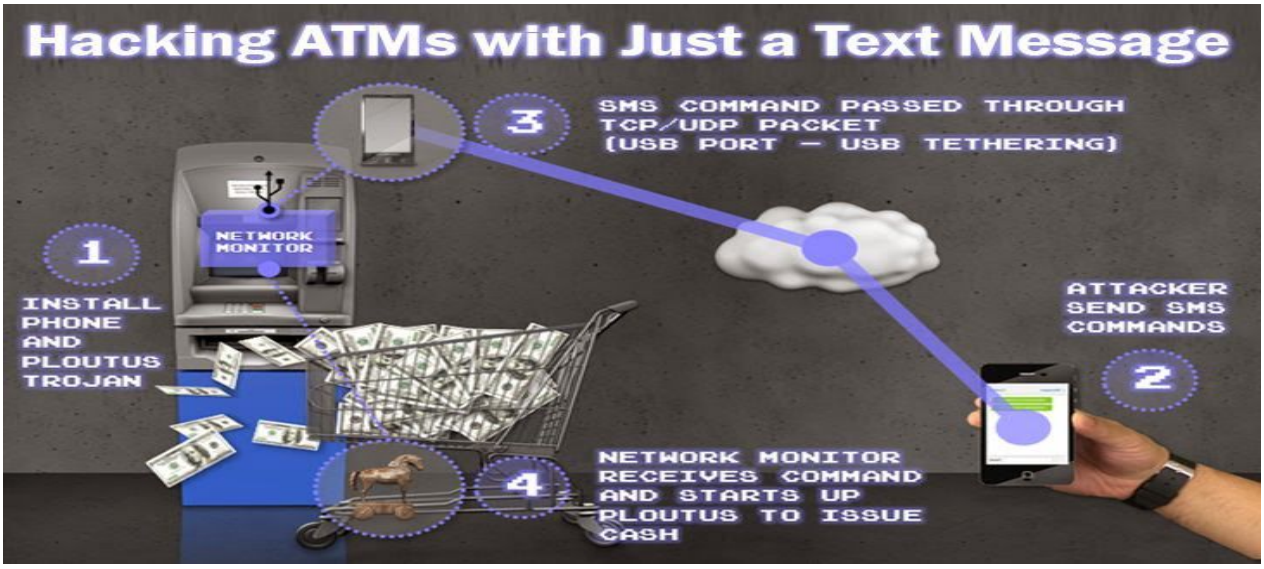


Growth of ATMs

In 2009, Retail Banking Research's "Global ATM Market and Forecasts to 2013" study predicted that the global ATM installed base would reach 2.5 million installations by 2013. With the number sitting at more than 2.3 million, that forecast appears to be right on track. RBR's most recent report puts the number of installed units at 3.4 million by 2017. This corroborates my own 10-year prediction back in 2007 that we would double the 1.56 million machines then in existence. Let's hope we're all correct and that we add another million or so ATMs to today's footprint! I agree with ATMIA CEO Mike Lee that the use of cash will continue to grow, fueling the aggressive expansion in our industry's collective crystal ball. The next five years will be exciting, indeed.

RESEARCH BACKGROUND

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. 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.



II. HARDWARE DESIGN

The S3C2440 chip is used as the core of entire hardware. The modules of LCD/Touch-screen, keyboard, fingerprint recognition, GSM Module are connected with the core S3C2440.The SRAM and FLASH are also embedded in this system.The system consist of following modules :-

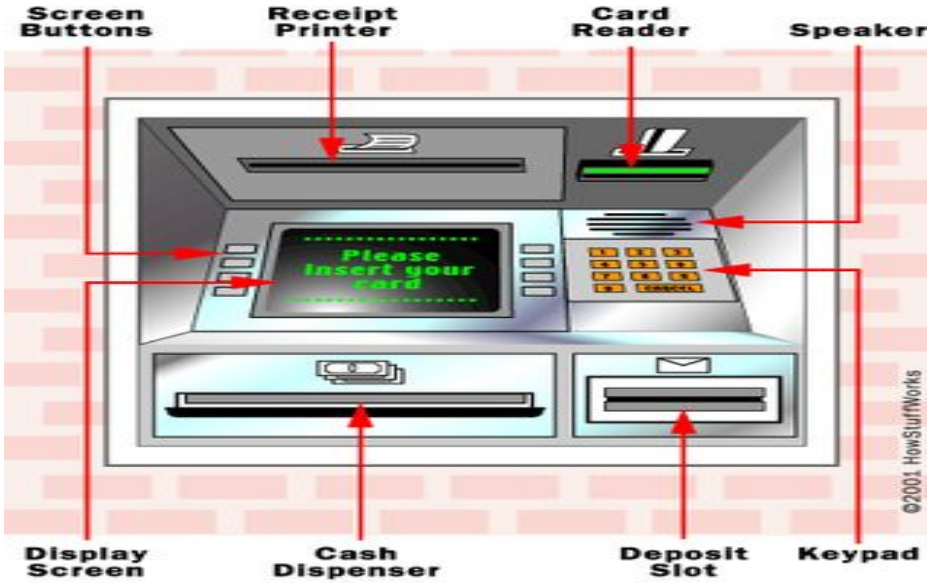
1.LCD module: The OMAP5910 is used as LCD module in LCD controller, it supported 1024*1024 images of 15 gray-scale or 3375 colours.

2. Keyboard/Touch-Screen module: It is used for inputting passwords.

3.Fingerprint recognition module: FIM3030 fingerprint module is used for recognition of is used for recognition of fingerprints. This module uses optical sensor for capturing and detecting of fingerprint images.

4.GSM Modem: A GSM modem(SIM 300) provides an interface that allows sending and receiving messages over the modem interfaces.

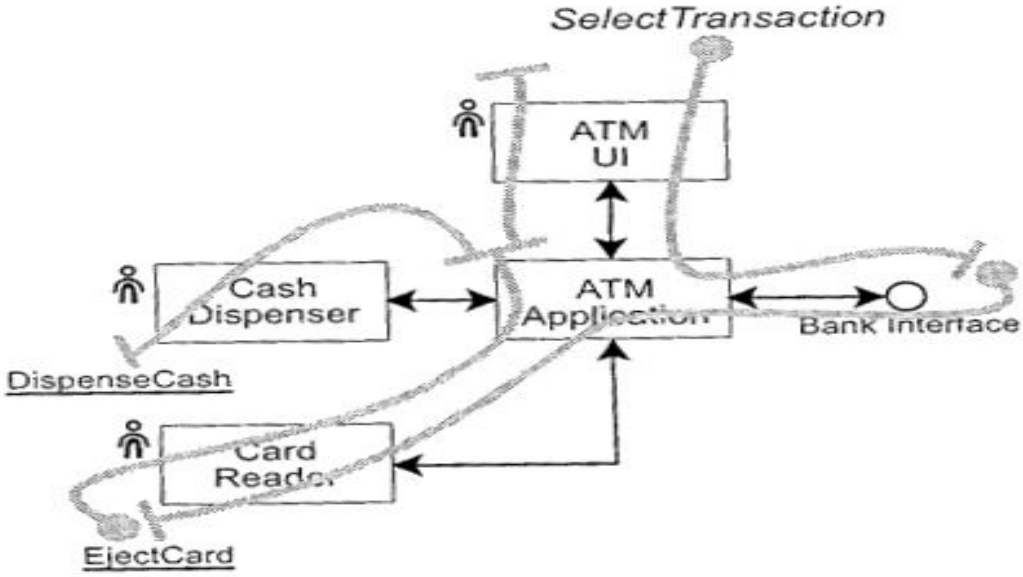
Figure1:- BLOCK DIAGRAM ATM SCURITY SYSTEM Before providing ATM access, the fingerprint module will compare scanned fingerprint with fingerprint taken at the time of opening account, if the figure print is correct 4 digit OTP is send to registered mobile number of user. The block diagram of hardware architecture is shown in figure



III. SOFTWARE DESIGN

The system operates in below two modes. Admin mode: In this mode the user finger print and mobile number are collected and saved at the time of opening the account.

User mode: In this mode the user finger print is validated with saved fingerprint for the identification which is required to perform transactions. This software system is designed as follows: first of all the Linux kernel and the File systems are loaded into the ARM 9 controller.In next step, the system is initialized to check specific task, such as checking ATM terminal, GSM module and so on, and then each module is reset for ready to run commands. Before accessing ATM system, the mobile number and fingerprint of the customer are needed to be authenticated.



IV. ATM SECURITY OVERVIEW

The cash in transit or stored in the ATM safe has been the asset traditionally targeted by ATM criminals, sometimes in rather violent ways. However, in the last years, attackers have turned their attention equally to soft assets present in the ATM, such as PINs and account data. Criminals use this stolen information to produce counterfeit cards to be used for fraudulent transactions—increasingly around the world—encompassing ATM withdrawals, purchases with PIN at the point of sale, and purchases without PIN in card-not-present environments. PINs and account data are assets belonging to cardholders and issuers. They are inevitably in "clear" form at the ATM, when the card and PIN are entered. By attaching, for example, a pinhole camera and a skimmer to the ATM, a criminal can steal PINs and account data before they can be securely processed by the ATM. These attacks require a relative low attack potential, in terms of both skills and material that is commercially available. The latest generations of skimmers and cameras are unnoticeable to untrained eyes and can be quickly installed and removed from the ATM without leaving any trace. In high traffic ATMs, dozens of PINs and associated account data sets can be stolen in a few hours.

V. BIOMETRICS ATMs

- Biometrics refers to the automatic identification of a person based on his physiological/behavioral characteristics.
- Various types of biometric systems are being used for real time identification;most popular are based on face recognition and finger print matching.

VI. WHY USING IT

1. Environmental Concerns
2. Security Concerns

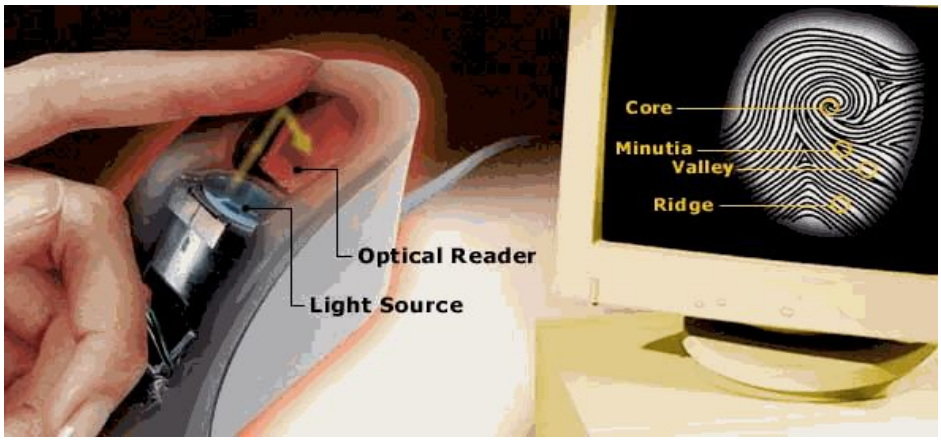
1. Envirormental Concerns:

- In conventional ATMs – PIN is needed
- PIN comes in an envelope which contains 2 sheets of paper and between this sheets secret code is marked
- RBI report says – 25000 new accounts are opened daily
- On yearly basis, a lot of paper is required – leads to cutting of trees

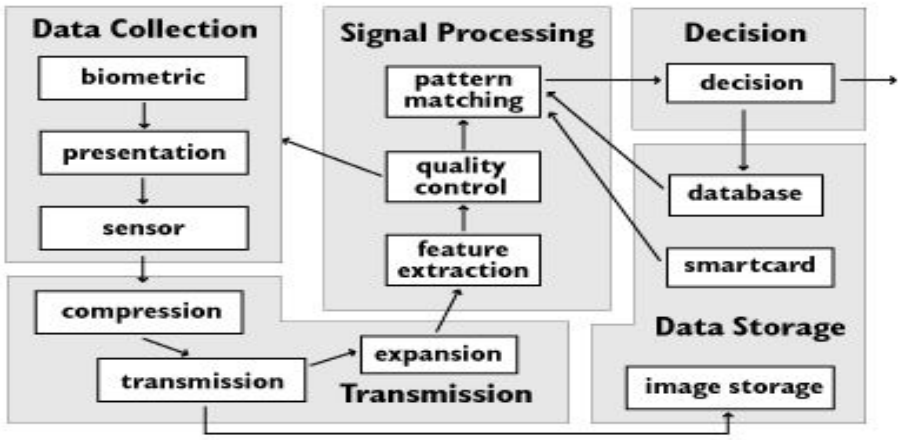
2. Security Concerns

- Anybody holding the card with PIN number known can operate
- No need to be the original owner of the card

- In Bio metric only the original card holder can operate



BIOMETRIC SYSTEM



VII. FINGERPRINT RECOGNITION PROCESS

The analysis of fingerprint matching needs the comparison of several features of the print pattern. This consists patterns which are aggregate characteristics of ridges & minutia points. These are unique features found within the patterns. It is important to know the structure and properties of human skin to successfully recognize the scanned fingerprint. In our proposed system the User's currently scanned fingerprint will be validated with fingerprint of user stored at the time of opening account. If authentication succeeds further access is given to customer.

Patterns

The three patterns of fingerprint ridges are i) arch, ii) loop & iii) whorl.

Arch: The ridges enter from side of the finger then rise in the center which forms an arc then exit the other side of the finger.

Loop: The ridges enter from side of a finger, forming curve then exit on that same side.

Whorl: Ridges form circularly around a central point on the finger. Fingerprint processing has three primary functions i) enrol, ii) search, iii) verify.
Enrollment captures fingerprint image from the sensor. Then image is processed, enhanced, and then compressed to form fingerprint template. Various filters filter the captured image and translate it to mathematical expression, making it difficult to steal template and directly recreate fingerprint image.Search compares scanned image to a list of enrolled fingerprint templates, through a series of screening processes. This algorithm reduces the list of templates to a manageable size. The templates that survive filtering are matched with currently scanned template and verification scores are provided. A score exceeding threshold score represents positive

VIII. 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 the world today, fingerprint is one of the essential variables used for enforcing security and maintaining a reliable identification of any individual. . Using the proper PIN gains access, but the user of the PIN is not verified. 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 using fingerprint identifier may solve this problem

IX. REFERENCE

[1] ENHANCED ATM SECURITY SYSTEM USING BIOMETRICS
Prof. Selina Oko , Department of Computer Science, Ebonyi State University Abakaliki, Nigeria and Jane Oruh Department of Computer Science, Michael Okpara University of Agriculture, Umudike, Nigeria

[2] 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

[3] Tom Harper Publisher, ATM MarketplaceExecutive summary-ATM Future Trends Report 2012

[4] ATM Security Using Fingerprint Biometric Identifer: An Investigative Study Moses Okechukwu Onyesolu Department of Computer Science Nnamdi Azikiwe University, Awka Anambra State, Nigeria. Ignatius Majesty Ezeani Department of Computer Science Nnamdi Azikiwe University, Awka Anambra State, Nigeria.

[6] A birthday present every eleven wallets? The security of customer-chosen banking PINs
Joseph Bonneau, Soren Preibusch, Ross Anderson

[7] Enhancing ATM Security using Fingerprint and GSM Technology V.Padmapriya Research Scholar SCSVMV University Enathur, kanchipuram S.Prakasam, Ph.D Asst. professor Department of CSA, SCSVMV University Enathur, kanchipuram

[8] Diebold I. (2002). ATM fraud and security: White Paper, New York.

[9] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing Security and Privacy in Biometrics-based Authentication Systems, IBM Systems Journal, vol. 40, no. 3, pp. 614-634, 2001.