Three Factor Authentication Schemes for the Automation of Inter-Networked banking and Teller Machine operations using Universal Subscriber Identification Modules

Sivasankar Bandaru*, Swapna. S**
*(M .Tech (WT), Aurora's Technological and Research Institute, JNTUH
Hyderabad, Andhra Pradesh, pin code-500035, India)
** (Assistant professor, IT Department, Aurora's Technological and Research Institute,
JNTUH Hyderabad, Andhra Pradesh, pin code-500035, India)

ABSTRACT

Automated teller machines (ATMs) are well known devices typically used by individuals to carry out a variety of personal and business financial transactions and/or banking functions. ATMs have become very popular with the general public for their availability and general user friendliness. ATMs are now found in many locations having a regular or high volume of consumer traffic. Various services and resources need protection from unauthorized use. Remote authentication is the most commonly used method to determine the identity of a remote client. This paper investigates a systematic approach for authenticating clients by three factors, namely password, smart card, and biometrics. Biometrics is the identification of humans by their characteristics or traits. A physiological biometric would identify by one's voice, Face, hand print or behaviour. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods.

Keywords— User authentication, Smart card, Face Recognition and security

I. INTRODUCTION

In a traditional password authentication scheme, a system server has to be able to authenticate a remote logon based on identity and password. [2] Password authentication protocols have two entities that share a password for the basis of authentication. Password authentication can be categorized into two types: weak-password authentication schemes and strong-password authentication schemes. strong-password authentication protocols have the advantages over the weak-password authentication schemes in that their computational overhead are lighter, designs are simpler, and the implementation are easier in the computational environments.

The security of accounts and passwords has always been a concern for the developers and users of Unix. When Unix was younger, the password encryption algorithm was a simulation of the M-209 cipher machine used by the U.S.

It has long been known that all a cracker need do to acquire access to a Unix machine is to follow two simple steps, namely:

1) Acquire a copy of that site's */etc/passwd* file, either through an unprotected *uucp* link, well known holes in *sendmail*, or via *ftp* or *tftp*

2) Apply the standard (or a sped-up) version of the password encryption algorithm to a collection of words, typically */usr/dict/words* plus some permutations on account and user names and compare the encrypted results to those found in the purloined */etc/passwd* file.[3]

A SIM card contains a unique serial number it reads the international mobile subscriber identity (IMSI), security authentication and ciphering information, temporary information related to the local network, a list of the services that the user has to access the two passwords: a personal identification number (PIN) for ordinary use and a personal unblocking code (PUK) for PIN unlocking.

Cryptographers have traditionally analysed the security of ciphers by modelling cryptographic algorithms as ideal mathematical objects. A modern cipher is conventionally modelled as a black box that accepts plaintext inputs and provides cipher text outputs. Inside this box, the algorithm maps the inputs to the outputs using a predefined function that depends on the value of a secret key. The black box is described mathematically and formal analysis is used to examine the system's security. In a modern cipher, an algorithm's security rests solely on the concealment of the secret key.[4] Smart cards serves ATM cards and mobile phone SIMs, authorization cards to provide high-security identification and access-control cards, Smart cards can be used as electronic wallets. The smart card chip can be "loaded" with funds to pay parking meters and vending machines. These Cryptographic protocols protect the exchange of money between the smart card and the accepting machines.

.

II. Functionality of Smart Card

Smart cards themselves usually are a small part of a much more complex system. There are usually complex networks of card terminals connecting to other backend host computers that process the information from transactions occurring at the card terminals. Companies investing in this infrastructure have a vested interest in standardizing the system components to guarantee the longevity of the system. Without standards, different manufacturers¢ components would not interoperate. The smart card systems would not be generally accepted because users would be forced to carry around many different, non-interoperable smart cards. This is an untenable situation for both users and manufacturers. [5]

Smart cards provide computing and business systems the enormous benefit of portable and secure storage of data and value. At the same time, the integration of smart cards into your system introduces its own security management issues, as people access card data far and wide in a variety of applications.

In a PKI system a Digital Signature verifies data at its origination by producing an identity that can be mutually verified by all parties involved in the transaction. A cryptographic hash algorithm produces a Digital Signature.

A. It ensure data privacy, by encrypting data
B. It ensures data integrity, by recognizing if data has been manipulated in an unauthorized way
C. Ensures data uniqueness by checking that data is "original", and not a "copy" of the "original". The sender attaches a unique identifier to the "original" data. This unique identifier is then checked by the receiver of the data.

Smart Card based Protocol provides three-factor authentication protocol involves a client C and a server S, and consists of five phases.
3-Factor-Initialization: S generates two system parameters PK and SK. PK is published in the system, and SK is kept secret by S. An execution of this algorithm is denoted by 3-Factor-Initialization (k) → (PK, SK), where K is system's security parameter.

3-Factor-Reg: A client C, with an initial password PW and biometric characteristics BioData, registers on the system by running this interactive protocol with the server S. The output of this protocol is a smart card SC, which is given to C. An execution of this protocol is denoted by

$$C[PW, BioData] \xleftrightarrow{3-\text{Factor}-\text{Reg}} S[SK] \to SC.$$

3-Factor-Login-Auth: This is another interactive protocol between the client C and the server S; this enables the client to login successfully using PW, SC, and BioData. An execution of this protocol is denoted by

$$C[PW,\ SC,\ BioData] \xleftrightarrow{3-\text{Factor}-\text{Login}-\text{Auth}} S[SK] \to \{1,0\}.$$

The output of this protocol is "1" (if the authentication is successful) or "0" (otherwise).
3-Factor-Password-Changing: This protocol enables a client to change his/her password after a successful authentication. The data in the smart card will be updated accordingly

3-Factor-Biometrics-Changing2: An analogue of password- changing is biometrics-changing, namely the client can change his/her biometrics used in the authentication, e.g., using a different finger or using iris instead of finger. While biometrics-changing is not supported by previous three-factor authentication protocols, we believe it provides the client with more flexibility in the authentication. [1]

III. Principal of Component Analysis (PCA) [6]:

Principal component analysis (PCA) creates new variables that consist of uncorrelated, linear combinations of the original variables. PCA is used to simplify the data structure PCA also known as Karhunen Loeve projection. PCA calculates the Eigen vectors of the covariance matrix, and projects the original data onto a lower dimensional feature space, which is defined by Eigen vectors with large Eigen values. PCA has been used in face representation and recognition where the Eigen vectors calculated are referred to as Eigen faces. In gel images, even more than in human faces, the dimensionality of the original data is vast compared to the size of the dataset, suggesting PCA as a useful first step in analysis. There are many approaches to face recognition ranging from the Principal Component Analysis (PCA) approach (also known as Eigen faces). Prediction through feature matching. The idea of feature selection and point matching has been used to track human motion. Eigen faces have been used to track human faces. They use a principal component analysis approach to store a set of known patterns in a compact subspace representation of the image space, where the subspace is spanned by the Eigen vectors of the training image set. It is one of the more successful techniques of face recognition and easy to understand and describe using mathematics. This method involves using Eigen faces [6]

IV. FACE RECOGNITION [7]:

The ability to recognize people by their facial characteristics Computers can conduct facial database searches and/or perform live, one-to-one or one-to-many verifications with unprecedented accuracy and split-second processing. Users can be granted secure access to their computer, mobile devices, or for online e-commerce, simply by looking into their Web camera.

The following details that can be shown

Security

- Military applications

Personal information access

- -ATM
- -Home access

Improved human machine interaction

Many face verification applications make it mandatory to acquire images with the same camera. However, some applications, particularly those used in law enforcement, allow image acquisition with many camera types. This variation has the potential to affect algorithm performance as severely as changing illumination. But, unlike the effects of changing illumination, the effects on performance of using multiple camera types have not been quantified. [7]

V. FIGURES

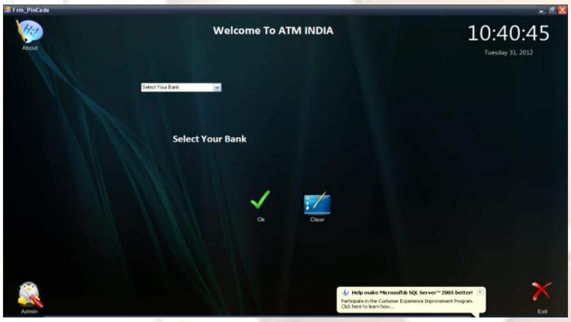

Frm_PinCode
Welcome To ATM INDIA
10:40:45
Tuesday 31, 2012
Select Your Bank
Help make Microsoft® SQL Server™ 2005 better!
Participate in the Customer Experience Improvement Program.
Click here to learn how....

Fig: 1 It shows the Bank Details

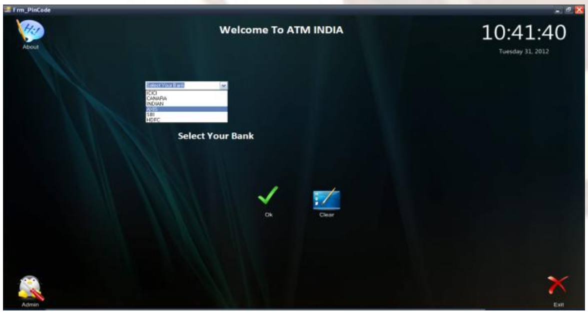

Frm_PinCode
Welcome To ATM INDIA
10:41:40
Tuesday 31, 2012
Select Your Bank

Fig: 2 it shows the types of Bank

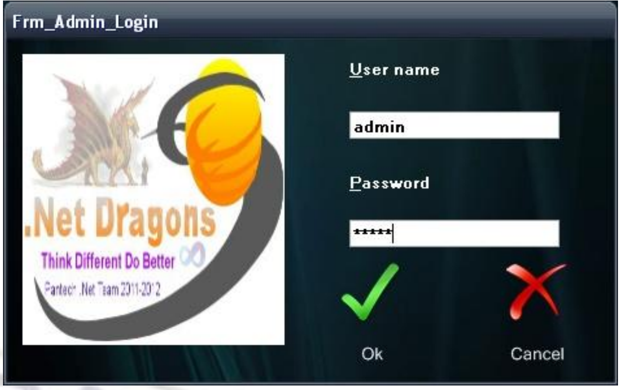
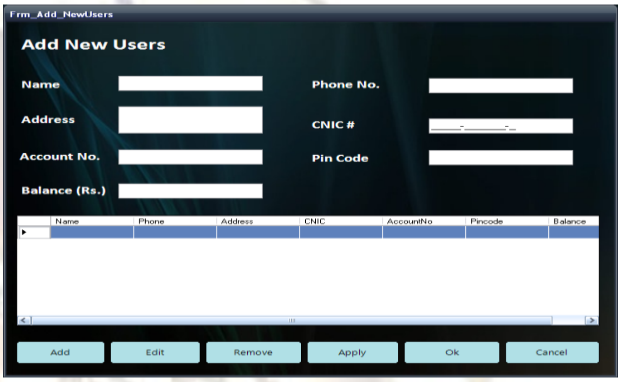

Frm_Admin_Login
User name: admin
Password: *****

Fig: 3 it shows the administration details


Frm_Add_NewUsers
Add New Users
Name
Address
Account No.
Balance (Rs.)
Phone No.
CNIC #
Pin Code

Name	Phone	Address	CNIC	AccountNo	Pincode	Balance

Fig:4 User Registration Form

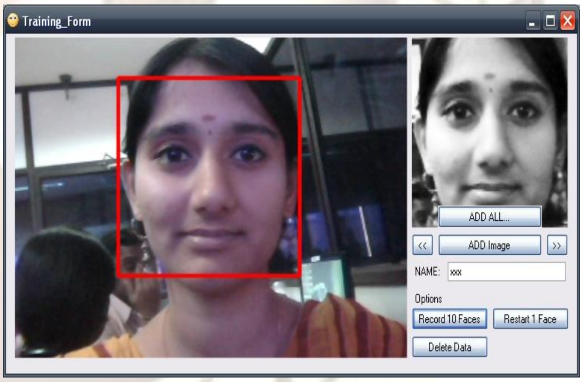

Training_Form
NAME: xxx

Fig:5 Capturing the image

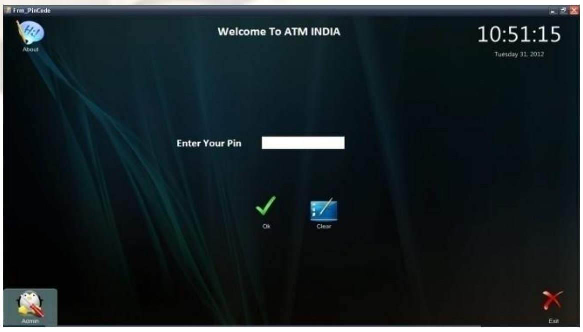

Frm_PinCode
Welcome To ATM INDIA
10:51:15
Tuesday 31, 2012
Enter Your Pin

Fig:6 User Enter the PIN Details

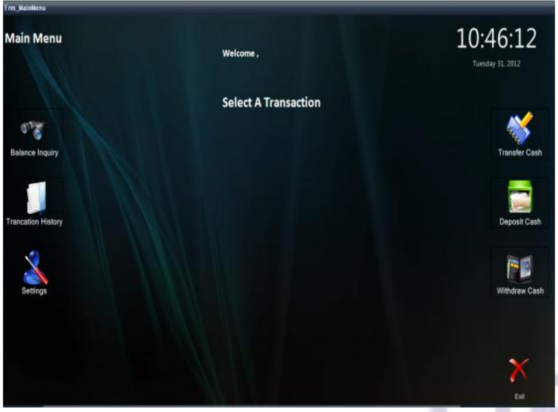


Fig:7 Transaction Details

VI. CONCLUSION:

ALL THE FUNCTIONS OF THE ATM, THE AUTHORS ARE NOW CONCENTRATING ON DEVELOPING THE INTENTION RECOGNITION, MOBILE BASED PROCESSING AND ALERT MODULE.

This paper presents a novel architecture that can be used as a means of interaction between mobile phone, ATM machine and a Banking application for the purpose of withdrawing cash. The proposed design; the secure M-cash withdrawal allows the use of mobile phones as a tool of interaction and provide flexibility through a robust identity management architecture. The first part of the architecture is the process of being implemented and all the process involved has been analysed and justified where possible.

VII. ACKNOWLEDGMENT

I would like to thanks some great mind without whom this research would have been adistant reality. I am totally by the side of these people. I would like to say thanks to my parents who support to me carry out my research without any hindrance. My deepest thanks to great person, my mentor Asst Prof. Swapna. S without whose ideas it was impossible.

REFERENCES

[1] Xinyi Huang, Yang Xiang, Member, IEEE, Ashley Chonka, Jianying Zhou, and Robert H. Deng, Senior Member, IEEE “A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems” IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 8, AUGUST 2011.

[2] C.H. Lin and Y.Y. Lai, “A Flexible Biometrics Remote User Authentication Scheme,” Computer Standards Interfaces, vol. 27, no. 1, pp. 19-23, Nov. 2004.

[3] D.V. Klein, “Foiling the Cracker: A Survey of, and Improvements to, Password Security,” Proc. Second USENIX Workshop Security, 1990.

[4] T.S. Messerges, E.A. Dabbish, and R.H. Sloan, “Examining Smart-Card Security under the Threat of Power Analysis Attacks,” IEEE Trans. Computers, vol. 51, no. 5, pp. 541-552, May 2002.

[5] Jorge Ferrari, Robert Mackinon, Sasan Poh and Lakshman Yathwara.” Smart card: Case Study” International Technical support Organization, October 1998.

[6] Srinivasulu Asadi, Dr.Ch.D.V.Subba Rao and V.Saikrishna “A Comparative study of Face Recognition with Principal Component Analysis and Cross-Correlation Technique” International Journal of Computer Applications (0975 – 8887) Volume 10– No.8, November 2010.

[7] P. J. Phillips, A. Martin C. L. Wilson and M. Przybocki, “An Introduction to Evaluating Biometric Systems,” IEEE Computer, Vol.33, No.2, Feb. 2000, pp. 56-63.

Authors Profile:

Sivasankar Bandaru is pursuing M. Tech in Web Technologies from Aurora’s Technological and Research Institute, JNTUH, A.P, INDIA. His research areas include Distributed System, and Computer networks.

S. Swapna received her M.Sc. Computer Science in 2007 from Reddy women’s College Narayanguda and M. Tech in Web Technologies from Aurora’s Technological and Research Institute, JNTUH, A.P, INDIA. Her area of expertise includes Operating system, Web Security and Database and Management System (DBMS), image processing. She is working as Assistant Professor in department of Information Technology at Aurora’s Technological and Research Institute, Hyderabad.