A Third Generation Design for the Automation of Inter-Networked Banking and Teller Machine Operations Using Universal Subscriber Identification Modules

Dr. Shaik Meeravali [#1], **K.Sudhakar** [*2], **Dayanand B. Jadhav** [#3]
[#1] *H.O.D., Professor, Dept. of ECE*
RRSCET,Muthangi(v),A.P.India.
[*2]*Assoc.Prof. Dept of ECE*
RRSCET, ,Muthangi(v),A.P.India.
[#3]*M.Tech. (E.S.) Student of RRSCET,*
Muthangi(v),A.P.India.

***Abstract*— The proposed system is designed on the basis of mobile SIM and the face-recognition technique i.e. image will be capture with the help of camera placed in the design . Firstly the SIM of mobile phone when inserted in the GSM unit of the ATM machine then the process will starts and the fitted camera will capture image of the user,then the information about the SIM card and the image captured will be match with the server database for the authenticated user. In the server database the information about SIM user character, behavior with different possible images, account information, ect. stores. When authenticated user then it asks the PIN number for next process. While if SIM and Image captured not match with the server database then the whole process will be terminated, thus the transaction will be secured.**

I. INTRODUCTION

Automated teller machines (ATMs) are well known devices typically used by individuals to carry out a business financial ,individual, transactions and/or banking functions. Therefore ATMs have become more popular.ATMs are now found in restaurants, supermarkets, Convenience stores, malls, schools, gas stations, hotels, work locations, banking centre, airports, entertainment establishments, transportation facilities and a myriad of in many other locations. ATMs are typically available to users on a continuous basis such that consumers have the ability to carry out their ATM financial transactions and/or banking functions at any time of the day and on any day of the week.

In the existing system the user should carry their ATM card without fail. But in many cases user forget it. So in the proposed system we designed a system which helps us to use the ATM machine without the ATM card.

Today security concerns are on the rise in all areas such as banks, governmental applications, healthcare industry, military organization, educational institutions, etc. Government organizations are setting standards, passing laws and forcing organizations and agencies to comply with these standards with non-compliance being met with wide-ranging consequences. There are several issues when it comes to security concerns in these numerous and varying industries with one common weak link being passwords.

Most systems today rely on static passwords to verify the user's identity. However, such passwords come with major management security concerns. Users tend to use easy-to-guess passwords, use the same password in multiple accounts, write the passwords or store them on their machines, etc. Furthermore, hackers have the option of using many techniques to steal passwords such as shoulder surfing, snooping, sniffing, guessing, etc. Several 'proper' strategies for using passwords have been proposed [1]. Some of which are very difficult to use and others might not meet the company's security concerns.

Two factor authentication using devices such as tokens and ATM cards has been proposed to solve the password problem and have shown to be difficult to hack. Two factor authentication also have disadvantages which include the cost of purchasing, issuing, and managing the tokens or cards. From the customer's point of view, using more than one two-factor authentication system requires carrying multiple tokens/cards which are likely to get lost or stolen.

Mobile phones have traditionally been regarded as a tool for making phone calls. But today, given the advances in hardware and software, mobile phones use have been expanded to send messages, check emails, store contacts, etc. Mobile connectivity options have also increased. After standard GSM connections, mobile phones now have infra-red, Bluetooth, 3G, and WLAN connectivity. Most of us, if not all of us, carry mobile phones for communication purpose. Several mobile banking services available take advantage of the improving capabilities of mobile devices. From being able to receive information on account balances in the form of SMS messages to using WAP and Java together with GPRS to allow fund transfers between accounts, stock trading, and

confirmation of direct payments via the phone's micro browser [12]. Installing both vendor-specific and third party applications allow mobile phones to provide expanded new services other than communication. Consequently, using the mobile phone as a token will make it easier for the customer to deal with multiple two factor authentication systems; in addition it will reduce the cost of manufacturing, distributing, and maintaining millions of tokens.

In this paper, we propose and develop a complete two factor authentication system using mobile phones instead of tokens or cards. The system consists of a server connected to a GSM modem and a mobile phone client running a J2ME application. Two modes of operation are available for the users based on their preference and constraints. The first is a stand-alone approach that is easy to use, secure, and cheap.

The second approach is an SMS-based approach that is also easy to use and secure, but more expensive. The system has been implemented and tested.

II. BACKGROUND

By definition, authentication is the use of one or more mechanisms to prove that you are who you claim to be. Once the identity of the human or machine is validated, access is granted. Three universally recognized authentication factors exist today: what you know (e.g. passwords), what you have (e.g. ATM card or tokens), and what you are (e.g. biometrics). Recent work has been done in trying alternative factors such as a fourth factor, e.g. somebody you know, which is based on the notion of vouching [10].

Two factor authentication [4] is a mechanism which implements two of the above mentioned factors and is therefore considered stronger and more secure than the traditionally implemented one factor authentication system. Withdrawing money from an ATM machine utilizes two factor authentication; the user must possess the ATM card, i.e. what you have, and must know a unique personal identification number (PIN), i.e. what you know.

Passwords are known to be one of the easiest targets of hackers. Therefore, most organizations are looking for more secure methods to protect their customers and employees. Biometrics are known to be very secure and are used in special organizations, but they are not used much in secure online transactions or ATM machines given the expensive hardware that is needed to identify the subject and the maintenance costs, etc. Instead, banks and companies are using tokens as a mean of two factor authentication.

A security token is a physical device that an authorized user of computer services is given to aid in authentication.

It is also referred to as an authentication token or a cryptographic token. Tokens come in two formats: hardware and software. Hardware tokens are small devices which are small and can be conveniently carried. Some of these tokens store cryptographic keys or biometric data, while others display a PIN that changes with time. At any particular time when a user wishes to log-in, i.e. authenticate, he uses the PIN displayed on the token in addition to his normal account password. Software tokens are programs that run on computers and provide a PIN that changes with time. Such programs implement a One Time Password (OTP) algorithm. OTP algorithms are critical to the security of systems employing them since unauthorized users should not be able to guess the next password in the sequence. The sequence should be random to the maximum possible extent, unpredictable, and irreversible. Factors that can be used in OTP generation include names, time, seed, etc. Several commercial two factor authentication systems exist today such as Best Buy's Bes Token [15], RSA's SecurID [14], and Secure Computing's Safeword [2].

Bes Token applies two-factor authentication through a smart card chip integrated USB token. It has a great deal of functionality by being able to both generate and store users' information such as passwords, certificates and keys. One application is to use it to log into laptops. In this case, the user has to enter a password while the USB token is plugged to the laptop at the time of the login. A hacker must compromise both the USB and the user account password to log into the laptop.

SecurID from RSA uses a token (which could be hardware or software) whose internal clock is synchronized with the main server. Each token has a *unique seed* which is used to generate a pseudo-random number. This seed is loaded into the server upon purchase of the token and used to identify the user. An OTP is generated using the token every 60 seconds. The same process occurs at the server side. A user uses the OTP along with a PIN which only he knows to authenticate and is validated at the server side. If the OTP and PIN match, the user is authenticated [8]. In services such as ecommerce, a great deal of time and money is put into countering possible threats and it has been pointed out that both the client and the server as well as the channel of communication between them is imperative [1].

In 2005 the National Bank of Abu Dhabi (NBAD) became the first bank in the Middle East to implement two factor authentication using tokens. It employed the RSA SecurID solution and issued its 19000 customers small hardware tokens [7, 14]. The National Bank of Dubai (NBD) made it compulsory for commercial customers to obtain tokens; as for personal customers the bank offered them the option to obtain the tokens [11]. In 2005, Bank of America also began providing two factor authentication for its 14 million customers by offering hardware tokens [5]. Many international banks also opted to provide their users

with tokens for additional security, such as Bank of Queensland, the Commonwealth Bank of Australia and the Bank of Ireland [3].

Using tokens involves several steps including registration of users, token production and distribution, user and token authentication, and user and token revocation among others [6]. While tokens provide a much safer environment for users, it can be very costly for organizations. For example, a bank with a million customers will have to purchase, install, and maintain a million tokens. Furthermore, the bank has to provide continuous support for training customers on how to use the tokens. The banks have to also be ready to provide replacements if a token breaks or gets stolen. Replacing a token is a lot more expensive than replacing an ATM card or resetting a password. From the customer's prospective, having an account with more than one bank means the need to carry and maintain several tokens which constitute a big inconvenience and can lead to tokens being lost, stolen, or broken. In many cases, the customers are charged for each token.

We propose a mobile-based software token that will save the organizations the cost of purchasing and maintaining the hardware tokens. Furthermore, will allow customers to install multiple software tokens on their mobile phones. Hence, they will only worry about their mobile phones instead of worrying about several hardware tokens.

III. DESIGN IMPLEMENTATION

In this paper, we propose a mobile-based software token system that is supposed to replace existing hardware and computer-based software tokens. The proposed system is secure and consists of three parts: (1) software installed on the client's mobile phone, (2) server software, and (3) a GSM modem connected to the server. The system will have two modes of operation:

• **Connection-Less Authentication System**: A onetime password (OTP) is generated without connecting the client to the server. The mobile phone will act as a token and use certain factors unique to it among other factors to generate a one-time password locally. The server will have all the required factors including the ones unique to each mobile phone in order to generate the same password at the server side and compare it to the password submitted by the client. The client may submit the password online or through a device such as an ATM machine. A program will be installed on the client's mobile phone to generate the OTP.

• **SMS-Based Authentication System**: In case the first method fails to work, the password is rejected, or the client and server are out of sync, the mobile phone can request the one time password directly from the server without the need to generate the OTP locally on the mobile phone. In order for the server to verify the identity of the user, the mobile phone sends to the server, via an SMS message, information unique to the user. The server checks the SMS content and if correct, returns a randomly generated OTP to the mobile phone. The user will then have a given amount of time to use the OTP before it expires. Note that this method will require both the client and server to pay for the telecommunication charges of sending the SMS message.

A. OTP Algorithm

In order to secure the system, the generated OTP must be hard to guess, retrieve, or trace by hackers. Therefore, its very important to develop a secure OTP generating algorithm. Several factors can be used by the OTP algorithm to generate a difficult-to-guess password. Users seem to be willing to use simple factors such as their mobile number and a PIN for services such as authorizing mobile micropayments [9]. Note that these factors must exist on both the mobile phone and server in order for both sides to generate the same password.

B. Client And Server Database Design

A J2ME program is developed and installed on the mobile phone to generate the OTP. The program has an *easyto- use* GUI that is developed using the NetBeans drag and drop interface. The program can run on any J2ME-enabled mobile phone. The OTP program has the option of (1) generating the OTP locally using the mobile credentials, e.g. IMEI and IMSI numbers, or (2) requesting the OTP from the server via an SMS message. The default option is the first method which is cheaper since no SMS messages are exchanged between the client and the server. However, the user has the option to select the SMS-based method.

In order for the user to run the OTP program, the user must enter his username and PIN and select the OTP generation method. The username, PIN, and generated OTP are *never* stored on the mobile phone.

If the user selects the connection-less method the username and PIN are used to locally generate the OTP and are discarded thereafter. The username and PIN are stored on the server's side to generate the same OTP.

A database is needed on the server side to store the client's identification information such as the first name, last name, username, pin, password, mobile IMEI number, IMSI number, unique symmetric key, and the mobile telephone number for each user. The password field will store the hash of the 10 minute password. It will not store the password itself. Should the database be compromised the hashes cannot be reversed in order to get the passwords used to generate those hashes. Hence, the OTP algorithm will not be traced.

IV. GETTING A DIGITAL IMAGE: THE FACIAL RECOGNITION SYSYTEM

Figure 1 below shows the typical way that a facial recognition system can be made operational

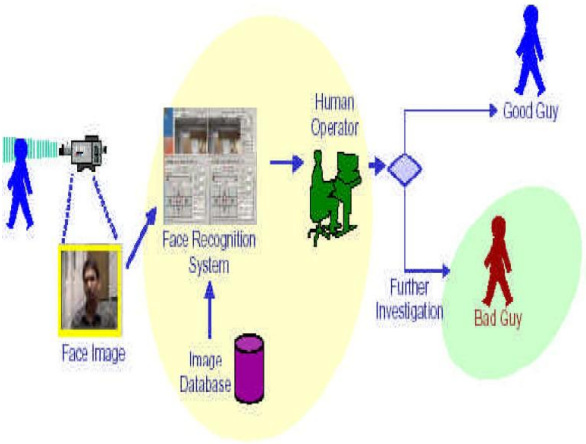

Figure 1: Overview of FRS

The first step is the capturing of a face image. This would normally be done using a still or video camera. The face image is passed to the recognition software for recognition (identification or verification). This would normally involve a number of steps such as normalizing the face image and then creating a 'template' of 'print' to be compared to those in the database. The match can either be a true match which would lead to investigative action or it might be a 'false positive' which means the recognition algorithm made a mistake and the alarm would be cancelled. Each element of the system can be located at different locations within a network, making it easy for a single operator to respond to a variety of systems.

V. PRINCIPAL COMPONENT ANALYSIS

Principal component analysis (PCA) involves a mathematical procedure which extracts facial features forrecognition, this approach transforms face images into a small set of characteristic feature images called eigenfaces.The first principal component accounts for as much of the variability in the data as possible, and each succeeding component accounts for as much of the remaining variability as possible. These methods capture the local facial features and their geometric relationships. They often locate anchor points at key facial features (eyes, nose, mouth, etc), connect these points to form a net and then measure the distances and angles of the net to create a unique face 'print'.

VI. IMAGE RECOGNITION VENDOR TEST

The medium size database consisted of number outdoor and video images from various sources. *Figure 2* below gives an indication of the images in the database. The top row shows nodal position (red dots) for the images and bottom row shows the various poses of images.

Figure 2: *Various poses images from the medium data base.*

With the very good images from the large database (37,437 images) the identification performance of the best system at rank one is 96% at a false accept rate of 1%.

A. The size of the database

The Face Recognition Vendor Test (FRVT) has recognized the face recognition in four technical areas. They are high resolution still imagery, 3D facial scans, multi sample still facial imagery and preprocessing algorithm (PCA) that compensate pose and illumination.

B. Individual's face

The method of defining the matrix varies according to the algorithm (the mathematical process used by the computer to perform the comparison). Here the part inside the oval is chosen and the other parts are rejected, artificial intelligence is used to simulate human interpretation of faces.

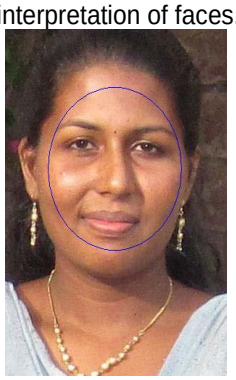

Figure3: Analytical oval face

In order to increase the accuracy and adaptability, some kind of machine learning of 3D face tracking, 3D face reconstruction has to be implemented.

VII .CONCLUSIONS

Today, single factor authentication, e.g. passwords, is no longer considered secure in the internet and banking world. Easy-to-guess passwords, such as names and age, are easily discovered by automated password-collecting programs. Two factor authentication has recently been introduced to meet the demand of organizations for providing stronger authentication options to its users. In most cases, a hardware token is given to each user for each account. The increasing number of carried tokens and the cost the manufacturing and maintaining them is becoming a burden on both the client and organization. Since many clients carry a mobile phone today at all times, an alternative is to install all the software tokens on the mobile phone. This will help reduce the manufacturing costs and the number of devices carried by the client .

Our paper has proposed a method of efficient 3D head tracking technique to overcome the consequence. Certain applications of face recognition technology are now cost effective, reliable and highly accurate. Face recognition technology can be used worldwide to access buildings, however it can be used in ATMs, which would help address potential security threats in near future.

References

[1] A. Jøsang and G. Sanderud, "Security in Mobile Communications: Challenges and Opportunities," in Proc. of the Australasian information security workshop conference on ACSW frontiers, 43-48, 2003.

[2] Aladdin Secure SafeWord 2008. Available at http://www. securecomputing.com/index.cfm?skey=1713

[3] A. Medrano, "Online Banking Security – Layers of Protection," Available at http://ezinearticles.com/?Online-Banking-Security---Layers-of-Protection&id=1353184

[4] B. Schneier, "Two-Factor Authentication: Too Little, Too Late," in Inside Risks 178, Communications of the ACM, 48(4), April 2005.

[5] D. Ilett, "US Bank Gives Two-Factor Authentication to Millions of Customers," 2005. Available at http://www.silicon.com/ financialservices/0,3800010322,39153981,00.htm

[6] D. de Borde, "Two-Factor Authentication," Siemens Enterprise Communications UK- Security Solutions, 2008. Available at http://www.insight.co.uk/files/whitepapers/Twofactor%20authentication%20(White%20paper).pdf

[7] A. Herzberg, "Payments and Banking with Mobile Personal Devices," Communications of the ACM, 46(5), 53-58, May 2003.

[8] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo and M. Yung, "Fourth- Factor Authentication: Somebody You Know," ACM CCS, 168-78. 2006.

[9] NBD Online Token. Available at http://www.nbd.com/NBD/ NBD_CDA/CDA_Web_pages/Internet_Banking/nbdonline_topbanner

[10] N. Mallat, M. Rossi, and V. Tuunainen, "Mobile Banking Services," Communications of the ACM, 47(8), 42-46, May 2004.

[11] "RSA Security Selected by National Bank of Abu Dhabi to Protect Online Banking Customers," 2005. Available at http://www.rsa.com/press_release.aspx?id =6092

[12] R. Groom, "Two Factor Authentication Using BESTOKEN Pro USB Token." Available at *http://bizsecurity.about.com/ od/mobilesecurity/a/twofactor.htm*

[13] Sha4J. Available at *http://www.softabar.com/home/content/ view/46/68/*

[14] SMSLib. Available at *http://smslib.org/*

[15] Faune Hughes, Daniel Lichter,Richard Oswald, and Michael Whitfield ,Face Biometrics:A Longitudinal Study, Seidenberg School of CSIS,Pace University, White Plains,NY 10606,USA.

[16] GaryG.Yen, Nethrie Nithianandan, Facial Feature Extraction Using Genetic Algorithm, Intelligent Systems and Control Laboratory School of Electrical and Computer Engineering. Oklahoma State University, Stillwater, OK 74074-5032, USA.

[17] D.L. Jiang, Y.X. Hu, S.C. Yan, H.J. Zhang, "Efficient 3D Reconstruction for Face Recognition", 0031_3203/2004 Pattern recognitionsociety:doi:10.1016/j.patcog.2004.11.004

[18] Animetrics offers FaceR™ CredentialME service on Sprint 3G and 4G networksAugust 12th, 2010

[19] Zigelman, G., Kimmel, R., Kiryati, N. Texture mapping using surface flatten-ing via multi-dimensional scaling, IEEE Trans. Visualization and Comp. Graphics, 8, pp. 198-207 (2002).

[20] T. F. Cootes, C. J. Taylor, D. Cooper, and J. Graham. Active shape models - their training and application. CVIU, 61(1):38–59, Jan. 1995.

[21] C. Vogler, Z. Li, A. Kanaujia, S. Goldenstein, and D. Metaxas. The best
of both worlds: Combining 3d de-formable models with active shape models. ICCV 2007.

[22] P. Mordohai and G. Medioni. Tensor Voting: A Perceptual Organization Approach to Computer Vision and Machine Learning. Morgan and Claypool Publishers, 2007.

[23] X. Pennec. Intrinsic statistics on riemannian manifolds: Basic tools for geometric measurements. Journal of Mathemat-ical Imaging and Vision, 25(1):127–154, July 2006.

[24] L. Gu and T. Kanade. 3d alignment of face in a single image. CVPR 2006, pp. 1305–1312.