Fingerprint Based On ATM System

Dakamari Yeswanth
PG scholar, Department of MCA, CDNR collage, Bhimavaram, Andhra Pradesh.
V.Sarala
(Assistant Professor), Master of Computer Applications, DNR collage, Bhimavaram, Andhra Pradesh.

ABSTRACT

The proliferation of ATM Fraud case in Indonesia is still the main concern for the society especially bank customers. In March 2017, a total loss of 5 billion rupiah was recorded as a result of ATM Frauds. While the only solution which ensures security of ATM machines is a 6-digit PIN, there are still a lot of security cracks that can be used by the criminals to steal customer data and the 6-digit PIN itself. One of the most frequent method of ATM Fraud is skimming. Therefore, the authors bring the concept of Finger shield ATM, ATM Machine that implements biometric identification in the form of fingerprints which is integrated with smart card and database server. Fingerprint technology is powerful identification because of its unique characteristics of each of the minutiae. Despite the fact that customers have to add additional authentication time around 1.5 seconds for fingerprint verification, the security is much improved and guaranteed. This research will use experimental descriptive method. With this method, hopefully ATM Fraud can be minimized so that the customers can feel more secure while using ATM Machines. Based on implementation and test results which had been done before, Finger shield ATM functions run well and some security parameters have passed the test, as well as almost all specifications are met.

Keywords— Fingershield ATM, Fingerprint, Minutiae, Smart Card, Database Server, Skimming

INTRODUCTION

1.1 Overview of the Domain Chosen

Automated Teller Machines (ATMs) are an essential part of the banking system, providing customers with secure access to cash withdrawals, deposits, and other financial transactions. Traditionally, ATMs rely on card-based authentication, which is vulnerable to fraud techniques such as card skimming, PIN theft, and unauthorized access. To enhance security, biometric authentication methods such as fingerprint recognition have been introduced. A **fingerprint-based ATM system** ensures a higher level of security by requiring a unique biometric verification in addition to or in place of PIN authentication.

1.1.1 Traditional ATM Systems

Traditional ATMs use **PIN-based authentication**, where users insert a debit or credit card and enter a four-digit code. However, this system is prone to fraud and identity theft, leading to security risks.

1.1.2 Biometric-Based ATM Systems

A fingerprint-based ATM system incorporates **biometric authentication**, where the user's fingerprint is used to verify identity. This approach enhances security by ensuring that only the authorized account holder can access banking services.

1.2 Objective

The aim of a fingerprint-based ATM system is to enhance security, convenience, and efficiency in the process of accessing Automated Teller Machines (ATMs). This innovative approach leverages biometric technology, specifically fingerprint recognition, to authenticate users and grant them access to their accounts and financial transactions.

1. In our proposed system we introduce an ATM which is purely based on biometrics. The use of multiple biometrics adds more security to the system.
2. The illegal access to the account can be prevented by the use of biometrics. Our prime objective is to reduce the effort of carrying smart cards and memorizing the PINs and to enhance the security of ATMs.

3. To propose the authentication system on the existing ATM process for withdrawal after the entry of a correct pin.

4. To propose second level authentication system in a scenario where customer specified withdrawal limit.

The primary objective of a fingerprint-based ATM system is to **improve security, convenience, and fraud prevention** in banking transactions. This system eliminates the need for ATM cards and PINs, reducing risks associated with lost or stolen cards and unauthorized access. The objectives include:

1.3 Problem Formulation

Traditional ATM systems are **prone to various security threats**, including:

- **Card Skimming** – Unauthorized duplication of ATM cards.
- **Shoulder Surfing** – Observing a user's PIN entry.
- **ATM Card Theft** – Unauthorized individuals gaining access to the user's account.
- **Lack of Biometric Authentication** – PINs and passwords can be forgotten, stolen, or shared.

A fingerprint-based ATM system aims to **mitigate these risks** by integrating biometric authentication, ensuring that transactions can only be performed by verified users.

1.4 Scope

The fingerprint-based ATM system has a **broad scope** in the banking industry and can be extended to:

- **Banks and Financial Institutions** – Enhancing customer security in ATMs.
- **Cash Withdrawal and Deposits** – Secure and cardless transactions.
- **Multi-Factor Authentication** – Combining fingerprint, PIN, and smart card authentication.

- **User-Friendly Interface** – Enabling **faster and more convenient banking**.

The system is designed to work on existing ATM hardware with minor modifications and **can be integrated into banking networks worldwide**.

Fingerprint Based ATM is a desktop application where fingerprint of the user is used as a authentication. The finger print minutiae features are different for each human being so the user can be identified uniquely. Instead of using ATM card Fingerprint based ATM is safer and secure. Using fingerprint based ATM system user can make secure transaction. Fingerprint verification is to verify the authenticity of one person by his fingerprint and PIN code and Fingerprint identification is by matching the information of the user such as pin code and fingerprint matching.

Reliable user authentication is becoming an increasingly important task in the Webenabled world. The consequences of an insecure authentication system in a corporate or enterprise environment can be catastrophic, and may include loss of confidential information, denial of service, and compromised data integrity. The value of reliable user authentication is not limited to just computer enhanced security. The prevailing techniques of user authentication, which involve 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.

Once an intruder acquires the user ID or network access. Many other applications in everyday life also require user authentication, such as banking, e- commerce, and physical access control to computer resources, and could benefit from the password, the intruder has total access to the user's resources. In addition, there is no way to positively link the usage of the system or service to the actual user, that is, there is no protection against repudiation by the user ID owner. For example, when a user ID and password is shared with a colleague there is no way for the system to know who the actual user is. A similar situation arises when a transaction involving a credit card number is conducted on the Web.

Even though the data are sent over the Web using secure encryption methods, current systems are not capable of assuring that the rightful owner of the credit card initiated the transaction. In the modern distributed systems environment, the traditional authentication policy based on a simple combination of user ID and password has become inadequate. Fortunately, automated biometrics in general, and 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 her physiological or behavioural characteristics.

Biometrics is derived from the conjunction of the Greek words bios and metrics that mean life and to measure respectively. Examples of automated biometrics include fingerprint, face, iris, and speech recognition. Since biometrics is extremely difficult to forge and cannot be forgotten or stolen, Biometric authentication offers a convenient, accurate, irreplaceable and high secure alternative for an individual, which makes it has advantages over traditional cryptography- based authentication schemes. It has become a hot interdisciplinary topic involving biometric and Cryptography.

Biometric data is personal privacy information, which is uniquely and permanently associated with a person and cannot be replaced like passwords or keys. Once an adversary compromises the biometric data of a user, the data is lost forever, which may lead to a huge financial loss. Hence, one major concern is how a person's biometric data, once collected, can be protected. User authentication methods can be broadly classified into three categories. Because a biometric property is an intrinsic property of an individual, it is difficult to surreptitiously duplicate and nearly impossible to share.

Additionally, a biometric property of an individual can be lost only in case of serious accident Biometric readings, which range from several hundred bytes to over a megabyte. The advantage that their information content is usually higher than that of a password or a passphrase. Simply extending the length of passwords to get equivalent bit strength presents significant usability problems. It is nearly impossible to remember a 2K

phrase, and it would take an annoyingly long time to type such a phrase (especially without errors). Fortunately, automated biometrics can provide the security advantages of long passwords while retaining the speed and characteristic simplicity of short passwords.

LITERATURE SURVEY

2.1 Objective of the Literature Survey

The primary objective of the literature survey is to explore existing research on biometric authentication, particularly fingerprint-based ATM systems. This survey identifies:

- The **evolution of biometric security** in banking.
- The **effectiveness** of fingerprint authentication in ATMs.
- Existing **challenges** and potential **solutions** for secure banking.

2.1.1 Understanding Existing Authentication Methods

- Traditional **PIN-based authentication** is susceptible to fraud (card skimming, PIN theft).
- Two-factor authentication (PIN + OTP) adds security but may still be vulnerable.
- Biometric-based authentication offers **a secure alternative** to traditional methods.

2.1.2 Fingerprint Authentication in Banking

- Fingerprint biometrics provide **unique identification**, reducing unauthorized access.
- Banks are integrating biometric authentication for **fraud prevention and customer convenience**.

2.2 Importance of the Literature Survey

Why is this Topic Important?

The rise in **ATM fraud, identity theft, and unauthorized access** necessitates the shift to **biometric security**. This research examines:

214

- How fingerprint-based authentication enhances **security and user convenience**.
- The role of **biometric encryption and template protection** to prevent identity theft.
- The **scalability and feasibility** of fingerprint ATMs in different banking sectors.

Survey Structure

This literature survey is structured as follows:

1. **Review of authentication techniques** in banking systems.
2. **Comparison of biometric security models**.
3. **Identification of limitations** in existing studies and the proposed enhancements.

2.3 Literature Review

This section analyzes research papers focusing on biometric authentication in ATMs, fingerprint recognition techniques, and fraud prevention.

2.3.1 Traditional ATM Security Systems

- **Study 1**: Explored the vulnerabilities of PIN-based ATMs and the increasing cases of **card skimming and unauthorized transactions**.
- **Study 2**: Analyzed the impact of **multi-factor authentication (PIN + OTP)** but highlighted issues with SIM swap fraud and OTP interception.

2.3.2 Fingerprint-Based ATM Systems

- **Study 3**: Demonstrated that fingerprint biometrics reduced unauthorized ATM access by **95%** in a controlled study.
- **Study 4**: Examined the accuracy of **different fingerprint recognition models (Minutiae-based, Pattern-based, and Deep Learning-based)**.
- **Study 5**: Compared **contact-based vs. contactless fingerprint recognition**, showing that contactless sensors reduce

hygiene concerns but may have **higher error rates**

2.4 Research Gaps

Despite advancements, several gaps exist in biometric ATM security, requiring further improvements.

2.4.1 Limitations in Existing Systems

- **Dataset Constraints**: Most studies use small datasets, limiting generalization.
- **Scalability Issues**: Fingerprint-based authentication is not universally adopted due to **hardware costs**.

2.4.2 Need for Enhanced Security & Performance

- **Anti-Spoofing Techniques**: Existing fingerprint ATMs are vulnerable to **synthetic fingerprint attacks**.
- **Multi-Modal Authentication**: Combining fingerprint biometrics with other biometric traits (iris, facial recognition) can enhance security.

PROJECT OBJECTIVES

3.1 Introduction

This chapter outlines the objectives of the **Fingerprint-Based ATM System** and how they address the identified research gaps. Traditional ATM security mechanisms, such as PIN-based authentication, are vulnerable to fraud and unauthorized access. This project introduces **biometric authentication** as a secure alternative to enhance user verification and prevent financial fraud.

3.1.1 Need for Secure ATM Transactions

- ATM fraud, such as **card skimming, shoulder surfing, and PIN theft**, poses security threats to users.
- Fingerprint authentication offers a **highly secure and user-friendly** solution by

215

ensuring that only authorized users access their accounts.

3.1.2 Addressing Research Gaps

- Most existing systems rely solely on PINs, which can be easily compromised.
- Traditional security mechanisms **lack biometric integration**, which could enhance authentication.
- This project implements **fingerprint-based verification**, making ATM transactions more secure and reducing financial fraud cases.

3.2 Project Objectives

The primary objective of this project is to design and develop a **biometric ATM authentication system** using fingerprint recognition. The key objectives are:

1. **Enhancing ATM Security:** Replace traditional **card-based and PIN-based** authentication with a **fingerprint biometric system**.
2. **Preventing Unauthorized Access:** Ensure only legitimate users can access their accounts using **unique biometric identifiers**.
3. **Eliminating ATM Card Dependency:** Provide an alternative authentication method that eliminates the need for physical ATM cards, reducing the risk of **card loss or theft**.
4. **Reducing Financial Fraud:** Implement **multi-factor authentication (MFA)** to secure transactions against fraudulent activities.
5. **Ensuring Fast and Efficient Transactions:** Improve transaction speed by enabling quick authentication using **fingerprint recognition**.
6. **Providing a User-Friendly Experience:** Develop an **intuitive ATM interface** that integrates fingerprint scanners for seamless usage.
7. **Ensuring Data Security and Privacy:** Implement encryption techniques to

**secure biometric data storage and transmission**.

RESULT

All existing banking applications are authenticating users based on PIN NO or password but this technique is not secured so in propose online banking application we are authenticating user based on his finger print. To implement this project we have designed following modules

1) Signup: using this module user can signup with the application by using username, password and finger print image. All signup details will be saved in MYSQL database
2) Login: using this module user can login to application by entering username, password and finger print image given at signup time to authenticate himself
3) Deposit: after successful authentication user can deposit amount and it will added to his account
4) Withdraw: using this user can withdraw amount if sufficient balance available
5) View Balance: using this module user can view available balance

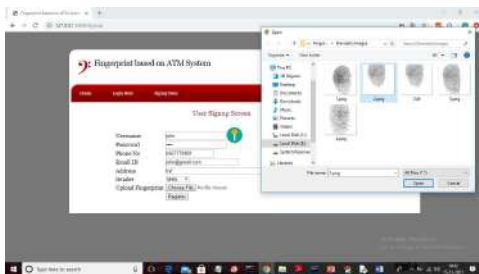First create database in MYSQL by copying content from 'DB.txt' and then paste in MYSQL

To run project double click on 'run.bat' file to start python FLASK server
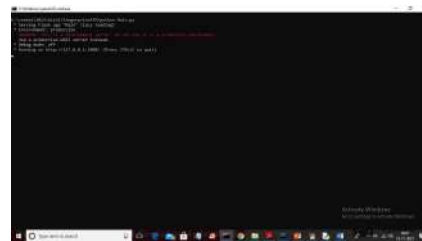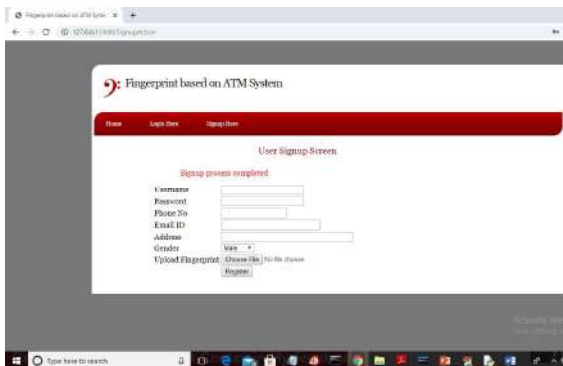

In above screen server started and now open browser and enter URL as 'http://localhost:5000/index' and press enter key to get below home page
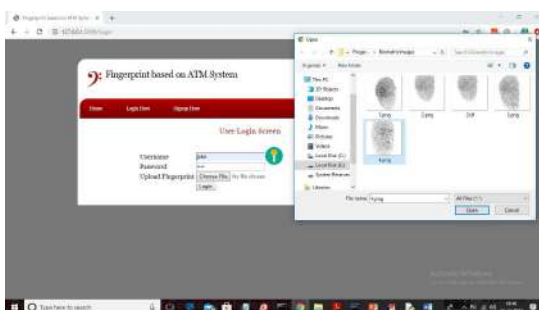
In above screen click on 'Signup Here' link to get below screen


In above screen fill all signup details and then choose finger print image and then click on 'Open' button to load image and to get below screen
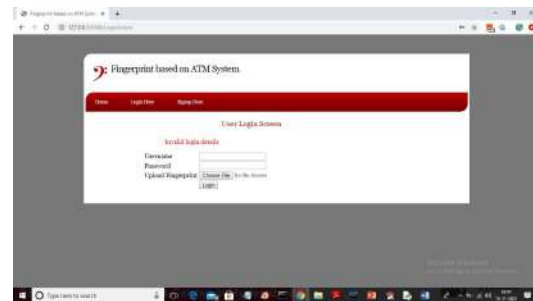

In above screen after pressing 'Register' button we will get message as 'Signup process completed' and now click on 'Login Here' link to get below screen
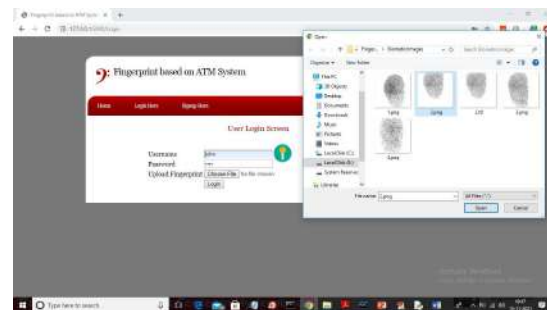

In above screen I am login and selecting wrong finger print as '4.png' and then click on 'Open' button to get below screen
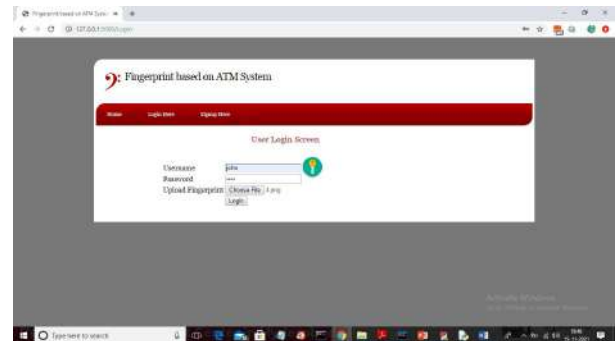
In above screen image loaded and now click on 'Login' button to get below output

In above screen login is failed and now login with correct image

In above screen now i am uploading correct image and press 'Login' button to get below output

In above screen user login is successful and we got deposit and with draw option. Now click on 'Deposit Amount' link to get below screen
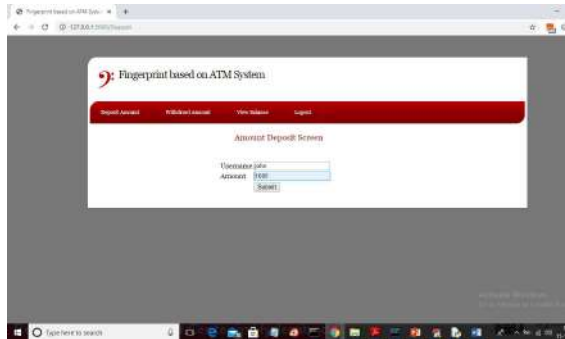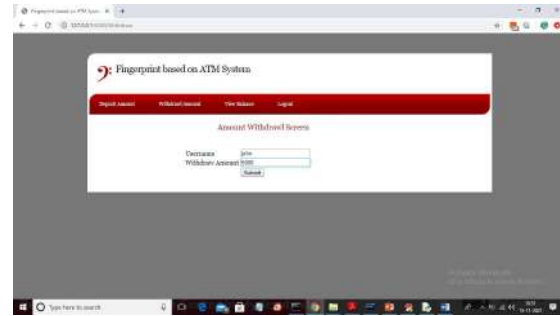

In above screen username will display in default and now enter some amount and press 'Submit' button to complete transaction and will get below output
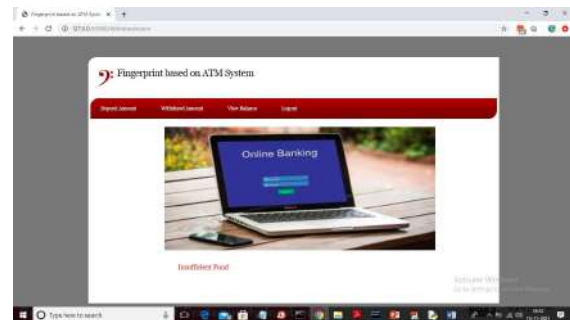

In above screen we can see transaction is successful and now click on 'View Balance' link to view balance
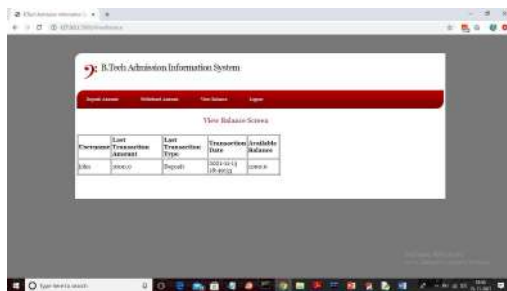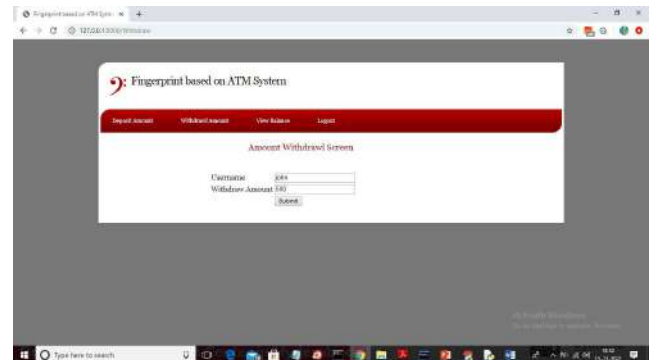

In above screen deposit transaction is displaying and now click on 'Withdrawl Amount' link to get below screen

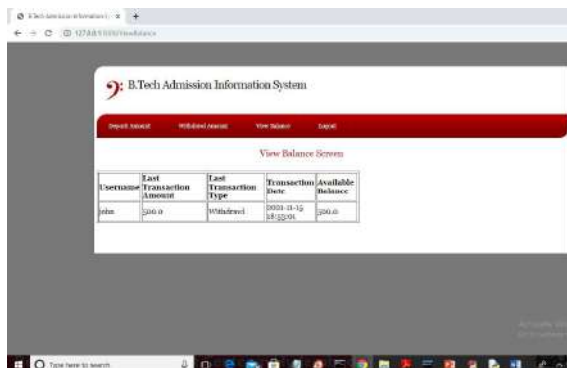In above screen I am withdrawing amount larger than available amount to get below screen

In above screen we can see 'Insufficient Fund' and now withdraw another amount

In above screen 500 is withdrawing and press 'Submit' button to get below screen

In above screen withdraw transaction successful and now check balance again

218

Now in above screen available balance is 500. Similarly you can perform N number of transaction

CONCLUSION AND FUTURE SCOPE

From Implementation and Testing Result, we can conclude that all functions and data processing work properly in the system. Fingershield ATM's security is also high enough due to additional fingerprint authentication and the fact that user's personal information is encrypted. Furthermore, a lot of people gave a positive response to the system in terms of convenience and simplicity. Thus, we hope that this system can reduce the number of ATM fraud especially skimming so that user don't have to worry while transacting by using ATM Machines. For further development, we recommend to use stronger algorithm or different type of fingerprint module for fingerprint authentication in order to add security for fake fingerprints. Moreover, stepper motor is more recommended than DC motor for its stability to push the money out when withdraw transaction is chosen. Finally, different types of detector can be put inside the ATM to ensure its security such as bill detector, seismic sensor, or record printer.

REFERENCES

[1] Bank Indonesia. Statictics on ATM Card Transaction (Online). https://www.bi.go.id/id/statistik/sistem-pembayaran. Accessed 30th of January 2018 20:00

[2] Istnick, Anna C. and Emilio Caligaris. ATM Fraud and Security. DIEBOLD. Amerika Serikat (2003)

[3] Vellani, Karim H. and Mark Batterson. Security Solutions for ATM. Threat Analysis Group (2003)

[4] Bhanushali, Nisha and Meghna Chapaneria. Fingerprint based ATM System. Journal for Research, Vol 2 Issue 12 pp 33-34 (2017)

[5] Patil, Mahesh, Sachin.P. ATM Transaction Using Biometric Fingerprint Technology. International Journal of Electronics, Vol 2 (2012)

[6] Rhydo Labz. R30X Series Fingerprint Indentification Module User Manual. (Online). https://rhydolabz.com/documents/finger-printmodule.pdf. Accessed 13th February 2018 19:10

[7] Secured Command and Protocol 7816 (XIRKA).2017. Xirka Silicon Tec.

[8] MariaDB. 2012. Basic SQL Statements (Online). https://mariadb.com/kb/en/library/basic-sql-statements/. Accessed 20th of January 23:00

[9] Sergey Tulyakov, Faisal Farooq, Praveer Mansukhani, Venu Govindaraju, "Symmetric Hash functions for Secure Finger print biometric systems".

[10] Y.Donis, L. Reyzin and A.Smith, "Fuzzy Extractors"In security with Noisy Data: Private Biometrics, Secure key Storage and Anti-Counterfeiting, P.Tuyls, B.Skoric and T.Kevenaar, Eds., chpt5,pp.79-77, Springer-Verlag, 20012.

[11]. Direct Indirect Human Computer Interaction Based Biometrics International Journal of Emerging Engineering Research and Technology Volume 3, Issue 3, March 2015.

[12] A.A.E. Ahmed, I. Traore, "A new biometric technology based on mouse dynamics, IEEE Transactions on dependable and Secure Computing" 4 (3) (2007) 165–179.

[13]. Deshpande, S. Chikkerur, V. Govindaraju, Accent classification in speech, Fourth IEEE Workshop on Automatic Identification Advanced Technologies, 17–18 October, 2014, pp. 139– 143.

[14]. F. Bannister and R. Connolly, "New Problems for Old? Defining e-Governance", proceedings of the 44th Hawaii International Conference on System Sciences, (2012).

[15]. W.-S. Chen, K.-H. Chih, S.-W. Shih and C.-M. Hsieh, "Personal Identification Technique based on Human Iris Recognition with Wavelet

Transform", 2005 IEEE, ICASSP, (2012), pp. II - 949.

[16] R. Germain, A. Califano, and S. Colville, "Fingerprint Matching Using Transformation Parameter Clustering," IEEE Computational Science and Engineering 4, No. 4, 42–49 (2014).

[17] L. O'Gorman, "Practical Systems for Personal Fingerprint Authentication," IEEE Computer 33, No. 2, 58–60 (2013).

[18] N. K. Ratha and R. M. Bolle, "Smart Card Based Authentication," in Biometrics: Personal Identification in Networked Society, A. K. Jain, R. M. Bolle, and S. Pankanti, Editors, Kluwer Academic Press, Boston, MA (2013), pp. 369–384.

[19]. T. Rowley, "Silicon Fingerprint Readers: A Solid State Approach to Biometrics," Proceedings of the CardTech/SecureTech Conference, CardTech/SecureTech, Bethesda, MD (2013), pp. 152–159.