ENHANCING ATM SECURITY WITH FINGERPRINT-BASED AUTHENTICATION

[1] A.Subhasini, Assistant Professor, Department of CSE, Chalapathi Institute of Technology, Guntur.
[2] Kadiyam Siva Ganesh, B.Tech, Department of CSE, Chalapathi Institute of Technology, Guntur.
[3] Gampala Tharun Kumar, B.Tech, Department of CSE, Chalapathi Institute of Technology, Guntur.
[4] Mallavarapu Saikumar, B.Tech, Department of CSE, Chalapathi Institute of Technology, Guntur.
[5] Dokku Vignesh, B.Tech, Department of CSE, Chalapathi Institute of Technology, Guntur.

Abstract: Identification and verification of a person today is a common thing; which may include door-lock system, safe box and vehicle control or even at accessing bank accounts via ATM, etc which is necessary for securing personal information. The conventional methods like ID card verification or signature does not provide perfection and reliability. The systems employed at these places must be fast enough and robust too. Use of the ATM (Automatic Teller Machine)which provides customers with the convenient banknote trading is facing a new challenge to carry on the valid identity to the customer. Since, in conventional identification methods with ATM, criminal cases are increasing making financial losses to customers.

1. INTRODUCTION

Biometrics is a technology that helps to make yourdata extremely secure, unique all the users by way of their personal physical characteristics. Biometric information can be used to perfectly identify people by using their fingerprint, face, speech, iris, handwriting, or hand geometry and so on. Using biometric identifiers offers several advantages over traditional and current methods .Tokens such as magnetic stripe cards, smart cards andphysical keys, can be stolen, lost, replicated, or left behind;passwords can be shared, forgotten, hacked or accidentallyobserved by a third party . There are two key functionsoffered by a biometric system. One technique isidentification and the other is verification. In this paper, weare concentrating on identifying and verifying a user byfingerprint recognition.A modern ATM is typically made up of the deviceslike CPU to control the user interface and devices related totransaction, Magnetic or Chip card reader to identify thecustomer, PIN Pad, Securecrypto-processor generallywithin a secure cover, Display to be used by the customerfor performing the transaction, Function key buttons,Record Printer to provide the customer with a record of theirtransaction, to store the parts of the machinery requiringrestricted access -Vault , Housing for aesthetics, Sensorsand Indicators. Fingerprint technology is the most widelyaccepted and mature biometric method.

2. LITERATURE SURVEY

TITLE: Biometric recognition: Securityand privacy concerns
AUTHOR: S. Prabhakar, S. Pankanti, and A. K. Jain

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. But how secure is biometrics? And what are the privacy implications?.

TITLE: **Handbook of Fingerprint Recognition**
AUTHOR: D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar

With their proven distinctiveness and stability over time, fingerprints continue to be the most widely used anatomical characteristic in systems that automatically recognize a person's identity. This markedly enhanced second edition provides in-depth coverage of the recent advances and practices in fingerprint recognition. Readers will find comprehensive and authoritative coverage of all the major concepts, topics, and systems and security issues associated with fingerprint recognition systems. Written with the same formula that made the success of the first edition, this unique professional reference includes state-of-the-art techniques in fingerprint matching, and covers developments in sensor technology, performance evaluation, international standards, and system security.

TITLE: **Biometrics: Personal Identification in Networked Society**.
AUTHOR: A. K. Jain, R. Bolle, and S. Pankanti, Eds.

Biomtrics: Personal Identification in Networked Society is a comprehensive and accessible source of state-of-the-art information on all existing and emerging biometrics: the science of automatically identifying individuals based on their physiological or behavioral characteristics.. "Biometrics: Personal Identification in Networked Society is an invaluable work for scientists, engineers,

application developers, systems integrators, and others working in biometrics.

TITLE: ATM Security Using Fingerprint Biometric Identifer: An Investigative Study.

AUHTOR: Moses OkechukwuOnyesolu, Ignatius MajestyEzeani

The growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, banks accounts and computer systems often use personal identification numbers (PIN's) for identification and security clearances. Conventional method of identification based on possession of ID cards or exclusive knowledge like a social security number or a password are not all together reliable. An embedded fingerprint biometric authentication scheme for automated teller machine (ATM) banking systems is proposed in this paper. In this scheme, a fingerprint biometric technique is fused with the ATM for person authentication to ameliorate the security level.

1. **TITLE: Fingerprint Matching**

AUTHOR: Anil K. Jain, Jianjiang Feng, Karthik Nandakumar

A fingerprint matching algorithm compares two given fingerprints and returns either a degree of similarity (without loss of generality, a score between 0 and 1) or a binary decision (mated/non-mated). Only a few matching algorithms operate directly on grayscale fingerprint images; most of them require that an intermediate fingerprint representation be derived through a feature extraction stage (refer to Chapter 3). Without loss of generality, hereafter we denote the representation of the fingerprint acquired during enrollment as the *template* (**T**) and the representation of the fingerprint to be matched as the *input* (**I**). In case no feature extraction is performed, the fingerprint representation coincides with the grayscale fingerprint image itself; hence, throughout this chapter, we denote both raw fingerprint images and fingerprint feature vectors.

3. EXISTING SYSTEM

The existing ATM system authenticates transactions via the card and PIN-based system. Thereafter, it grants access to bank customers to several services such as cash withdrawal and deposits, account to account transfers, balance enquiry, topup purchases and utility bills payment. The ATM system compares the PIN entered against the stored authorization PIN for every ATM users. If there is a match, the system authenticates die user and grants access to all the services available via the ATM. If there is a mismatch on the other hand, the user authentication process fails and the user is given two more opportunities to enter a correct PIN. If an incorrect PIN is entered for the third time, the card gets blocked and retained by the ATM.

. DISADVANTAGES OF EXISTING SYSTEM

- Security: Traditional ATM systems rely on PIN codes for security. However, PIN codes can be stolen or guessed, which can lead to fraudulent activities. Fingerprint-based systems, on the other hand, are much more secure as they are nearly impossible to fake or duplicate.
- Convenience: Fingerprint-based systems are more convenient for users as they eliminate the need to remember and enter PIN codes. This can save time and reduce the risk of forgetting or losing a PIN code.

4. PROPOSED SYSTEM

The proposed system is an improvement of the existing system, and it does not require card and PIN to operate. The proposed system work with biometric fingerprint only, the customer uses fingerprint at ATM and if matched correctly, the nall banks of the customer have account with appears, the customer will select the bank to transaction with, then select the account type with that bank, then chose to withdraw, check account balance and so on. Customer will now choose or select the bank he wants to withdraw money from and specify if the account is Current or Savings, this is a means of securing ATM transaction using biometric fingerprint. This proposed system has a lot of advantages over the existing Card and PIN method

ADVANTAGES

- Strong Authentication
- Our System replaces card system with physiological characteristics.
- Hidden cost of ATM Card Management cans be avoided.
- It’s ideal for rural masses 5.
- Useful for senior system because no need to carry cards and memorize passwords
- Due to bio metric system no one is able to access the other systems.
- User can change the authentication any time in home branch with few simple procedures.

SYSTEM ARCHITECTURE

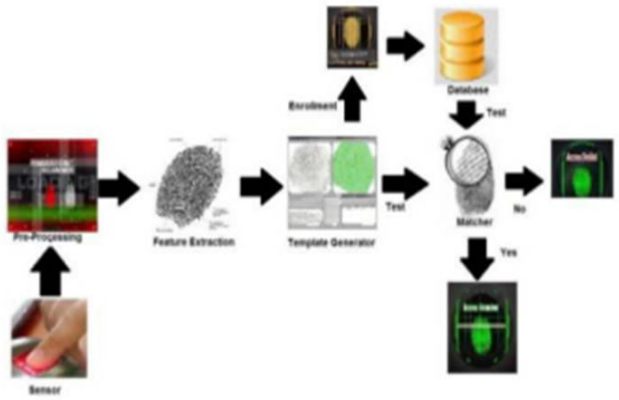

Fig 1: System Architecture

5. UML DIAGRAMS

5.1 CLASS DIAGRAM

The cornerstone of event-driven data exploration is the class outline. Both broad practical verification of the application's precision and fine-grained demonstration of the model translation into software code rely on its availability. Class graphs are another data visualization option.

The core components, application involvement, and class changes are all represented by comparable classes in the class diagram. Classes with three-participant boxes are referred to be "incorporated into the framework," and each class has three different locations:

• The techniques or actions that the class may use or reject are depicted at the bottom.

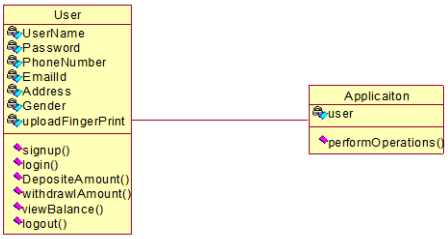

Fig 5.1 shows the class diagram of the project

5.2 USECASE DIAGRAM:

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

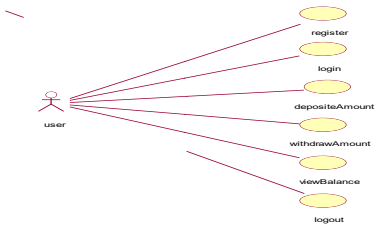

Fig 5.2 Shows the Use case Diagram

6.3 SEQUENCE DIAGRAM:

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

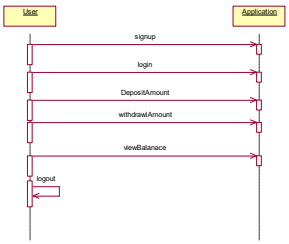

Fig 5.3 Shows the Sequence Diagram

6. RESULTS

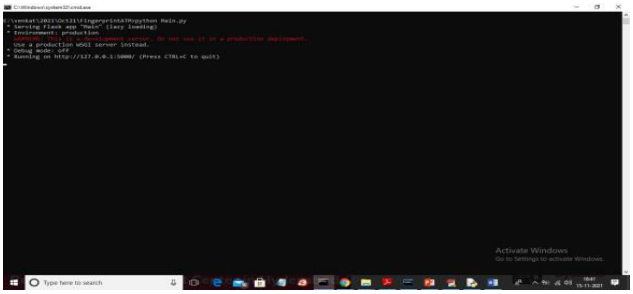

Fig 6.1 In above screen server started and now open browser and enter URL as ‘http://localhost:5000/index’ and press enter key to get below home page

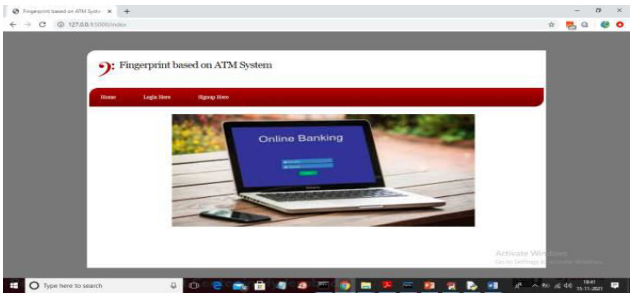

Fig 6.2 In above screen click on 'Signup Here' link to get below screen

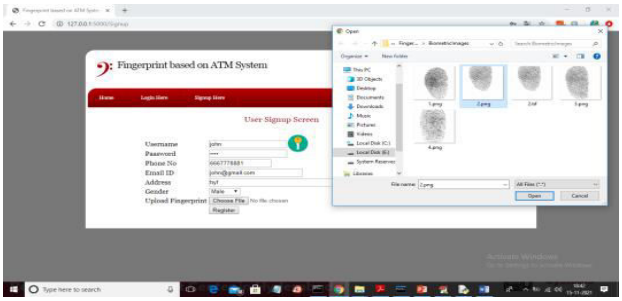

Fig 6.3 In above screen fill all signup details and then choose finger print image and then click on 'Open' button to load image and to get below screen

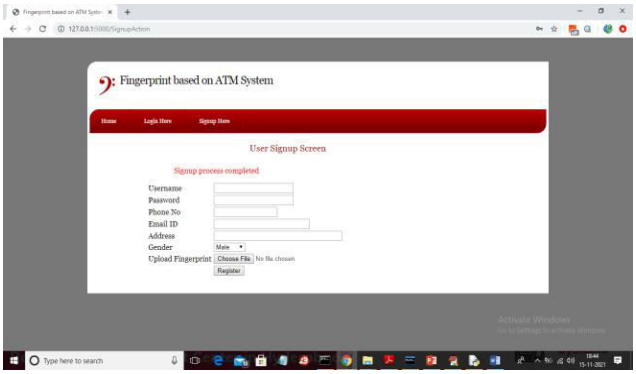

Fig 6.4 In above screen after pressing 'Register' button we will get message as 'Signup process completed' and now click on 'Login Here' link to get below screen

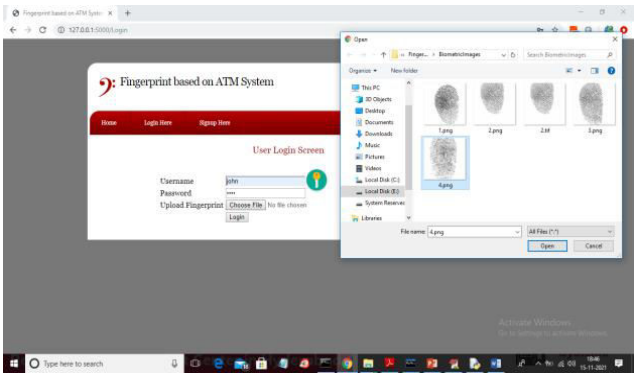

Fig 6.5 In above screen I am login and selecting wrong finger print as '4.png' and then click on 'Open' button to get below screen

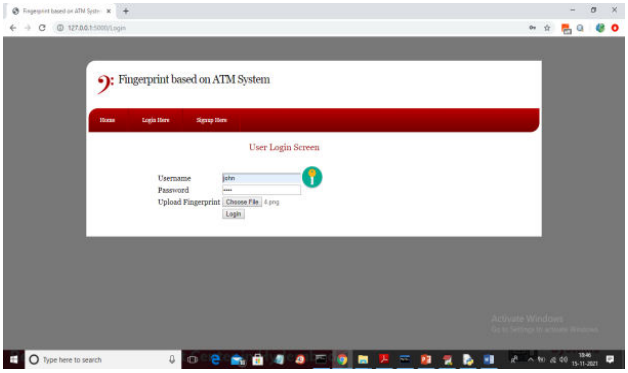

Fig 6.6 In above screen image loaded and now click on 'Login' button to get below output

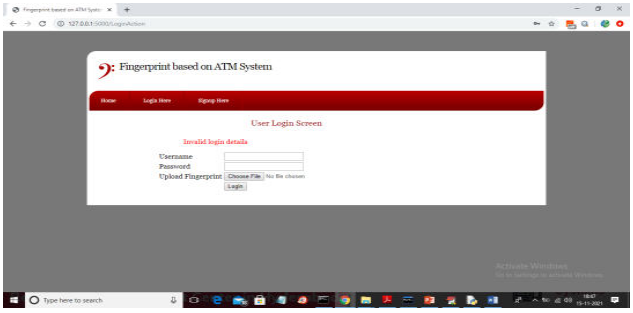

Fig 6.7 In above screen login is failed and now login with correct image

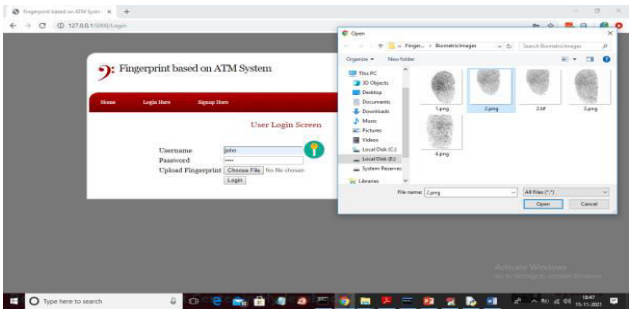

Fig 6.8 In above screen now i am uploading correct image and press 'Login' button to get below output

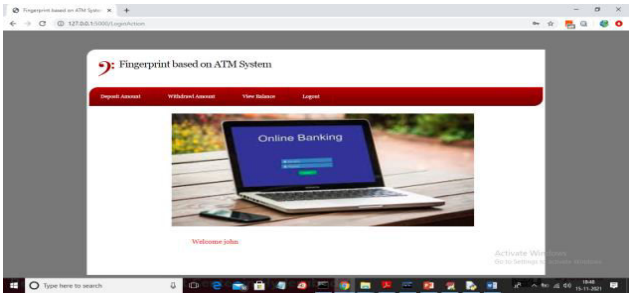

Fig 6.9 In above screen user login is successful and we got deposit and with draw option. Now click on 'Deposit Amount' link to get below screen

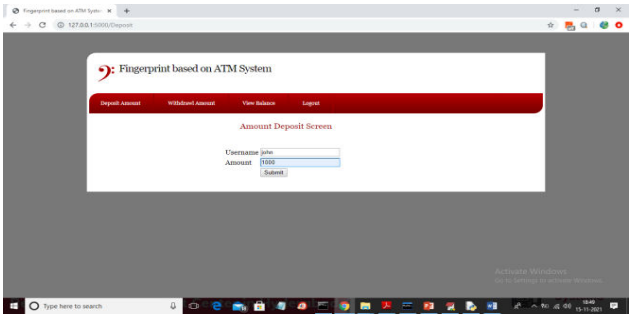

Fig 6.10 In above screen username will display in default and now enter some amount and press 'Submit' button to complete transaction and will get below output

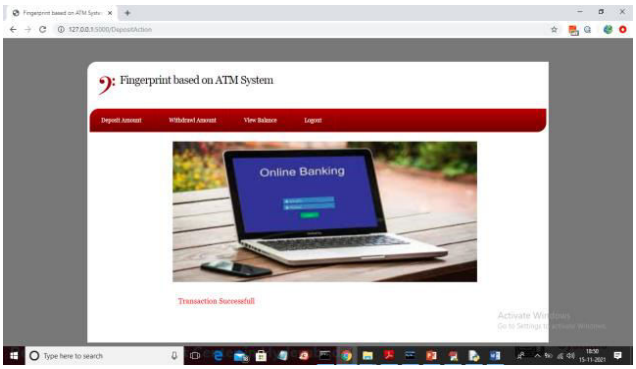

Fig 6.11 In above screen we can see transaction is successful and now click on 'View Balance' link to view balance

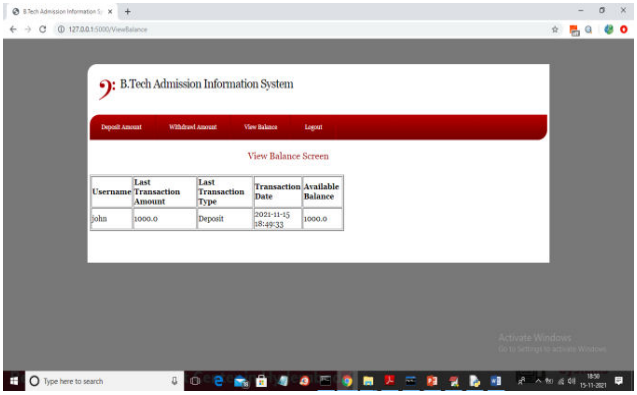

Fig 6.12 In above screen deposit transaction is displaying and now click on 'Withdrawl Amount' link to get below screen

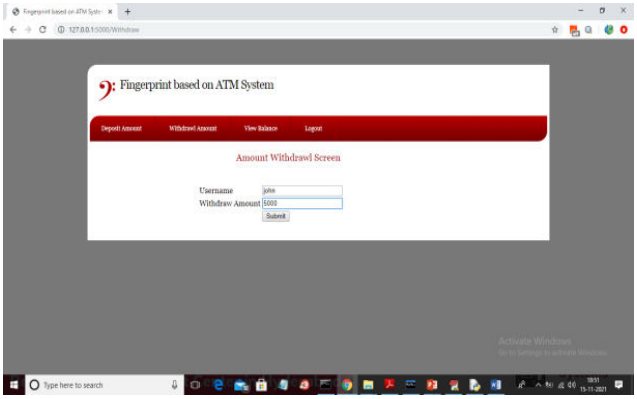

Fig 6.13 In above screen I am withdrawing amount larger than available amount to get below screen

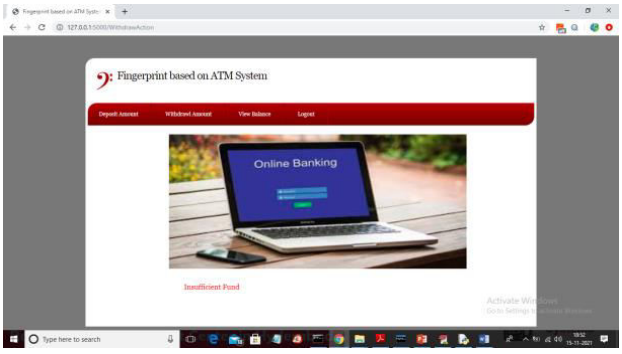

Fig 6.14 In above screen we can see 'Insufficient Fund' and now withdraw another amount

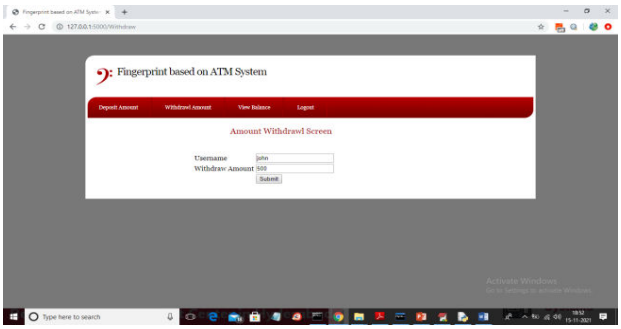

Fig 6.15 In above screen 500 is withdrawing and press 'Submit' button to get below screen

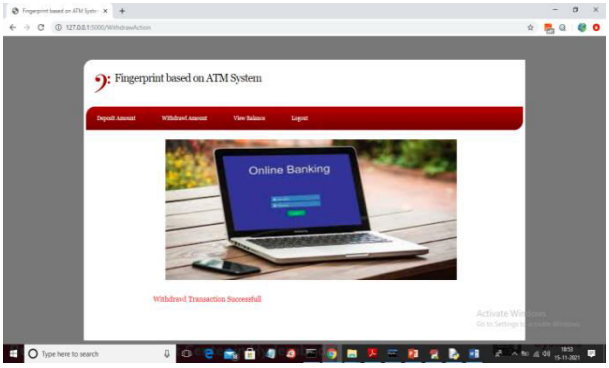

Fig 6.16 In above screen withdraw transaction successful and now check balance again

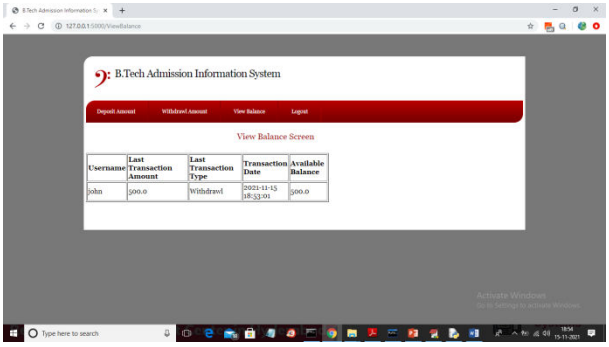

Fig 6.17 Now in above screen available balance is 500. Similarly you can perform N number of transaction

7. CONCLUSION

After testing the system developed, we came to know that ATM prototype can be efficiently used with finger print recognition. Since, password protection is not bypassed in our system, the fingerprint recognition done after it yielded fast response and is found to be of ease for use. Finger print images cannot be recreated from templates; hence no one can misuse the system. LPC2148 and FIM3030 provide low power consumption platform. Speed Of execution can be enhanced with the use of more sophisticated micro controller. The same hardware platform can be used with IRIS scanner to put forward another potential biometric security to the ATMs.

8. REFERENCES

[1] S. Prabhakar, S. Pankanti, and A. K. Jain,"Biometric recognition: Securityand privacy concerns," IEEE Security PrivacyMag., vol. 1, no. 2,pp. 33–42, 2003.

[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar,Handbook of Fingerprint Recognition. New York: Springer-Verlag, 2003.

[3] A. K. Jain, R. Bolle, and S. Pankanti, Eds.,Biometrics: Personal Identificationin NetworkedSociety. Norwell, MA: Kluwer, 1999.

[4] Moses OkechukwuOnyesolu, Ignatius MajestyEzeani, "ATM Security Using FingerprintBiometric Identifer: An Investigative Study",(IJACSA) International Journal of AdvancedComputer Science and Applications, Vol. 3, No.4,2012, pp. 68-72

[5] Anil K. Jain, Jianjiang Feng, Karthik Nandakumar,"Fingerprint Matching", IEEE ComputerSociety2010, pp. 36-44, 0018-9162/10.

[6] Pranali Ravikant Hatwar and Ravikant B Hatwar, BioSignal based Biometric Practices, International Journal of Creative Research Thoughts, Vol. 1, No. 4, pp. 1-9, 2013.

[7] Edmund Spinella, Biometric Scanning Technologies: Finger, Facial and Retinal Scanning, Available at: https://www.sans.org/readingroom/whitepapers/authenticat i on/biometricscanningtechnologies-finger-facial-retinal-sca nning-1177.

[8] Gu J, Zhou J, Zhang D.A combination model for orientation field of fingerprints. Pattern Recognition, 2004, 37:543-553.

[9] N. Selvaraj and G. Sekar, A Method to enhance the Safety Level of the ATM banking industry
using AES Algorithm, International Journal of Computer Applications, Vol. 3, No. 6, pp. 5-9, 2010.

[10] A. Haldorai and A. Ramu, Security and channel noise management in cognitive radio networks, Computers & Electrical Engineering, vol. 87, p. 106784, Oct. 2020. doi:10.1016/j.compeleceng.2020.106784

[11] A. Haldorai and A. Ramu, Canonical Correlation Analysis Based Hyper Basis Feedforward Neural Network Classification for Urban Sustainability, Neural Processing Letters, Aug. 2020. doi:10.1007/s11063-020-10327-3

[12] J. Yang N. Xiong, A.V. Vasilakos, Z. Fang, D. Park, X. Xu, S. Yoon, S. Xie and Y. Yang A Fingerprint Recognition Scheme supported Assembling Invariant

Moments for Cloud Computing Communications, IEEE Systems Journal, Vol. 5, No. 4, pp. 574-583, 2011.
[13] J. Leon G. Sanchez G. Aguilar, L. Toscano, H. Perez and J.M. Ramirez, Fingerprint Verification Applying Invariant Moments, Proceedings of IEEE International Midwest Symposium on Circuits and Systems, pp. 751-757, 2009.
[14] LO Gorman Overview of Fingerprint Verification Technologies, Information Security Technical Report, Vol. 3, No. 1, p. 21-32, 1998.
[15] G.B. Iwalokun O.C. Akinyokun, B.K. Alese and O. Olabode Fingerprint Image Enhancement: Segmentation to Thinning, International Journal of Advanced computing and Applications, Vol. 3, No. 1, pp. 15-24., 2012