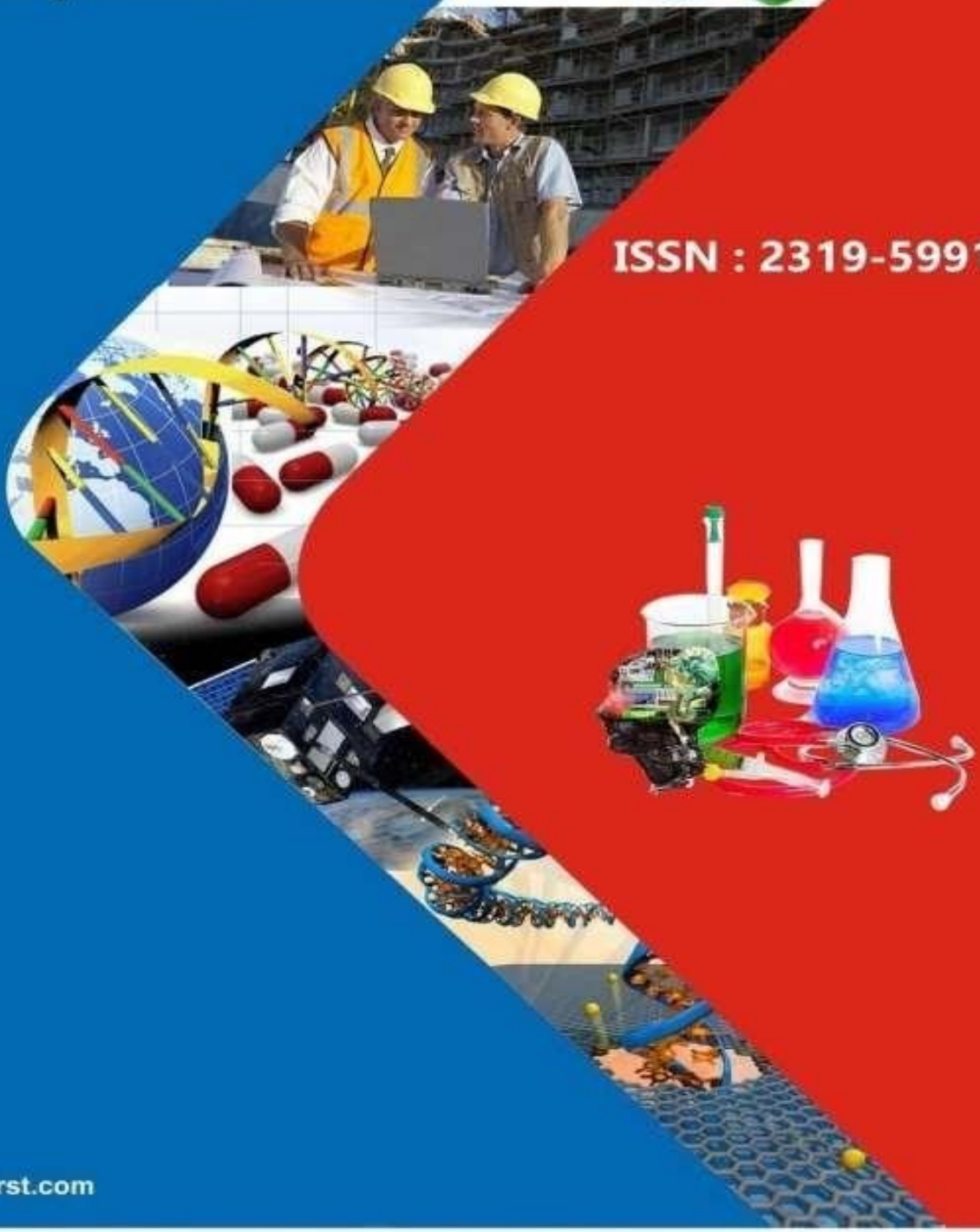
International Journal of Engineering Research and Science & Technology

IJERST

ISSN : 2319-5991



www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

https://doi.org/10.62643/ijerst.2024.v20.i3.pp232-237

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue 3, 2024

FINGERPRINT BASED ATM SYSTEM

[1]Dr K Venkata Naganjaneyulu,[2]T. Nalini Devi,[3]Shaik Asiya,[4]R. Swathi
[1]Professor,[234]Students
Department Of CSE
Malla Reddy Engineering College for Women

ABSTRACT

The project's overarching goal is to offer a safe banking system that uses fingerprints as an approved identification at ATMs and banks. The project's goal is to make online banking safer and more dependable for consumers by assigning a unique identity to each user using the FINGER PRINT identification system.

These days, it's normal practice to need authentication whenever you do anything involving sensitive information, such as opening a door, entering a safe, controlling a car, or even using an ATM to access your bank account. Traditional approaches, such as relying on a signature or ID card, fall short when it comes to providing absolute certainty. The systems used there need to be both quick and reliable. The new problem of validating the customer's identification is affecting the use of ATMs, which provide clients easy access to trade banknotes. Since criminal cases are on the rise due to traditional ATM identification procedures, consumers are losing money.

A desktop program that uses the user's fingerprint as authentication is called a fingerprint-based ATM. Each person's fingerprint has unique characteristics that allow for individual identification. I prefer not to use my ATM card. A better and more secure option is an ATM that uses fingerprint technology. You can stop worrying about misplacing your ATM card and stop carrying it about in your wallet. To complete any kind of financial transaction, all you need is your fingerprint. In order to proceed with more transactions, the user must first log in using his fingerprint and then input the PIN. Money may be withdrawn from the user's account. By providing the account number, users may send funds to several accounts. You need to specify the account you want to withdraw funds from and the amount you want to remove before you can proceed with the withdrawal.The user's ATM account must have sufficient funds in order to complete the transaction. The available balance in each user's account may be seen. Viewing the previous five transactions is a feature that the system offers to users.

I.INTRODUCTION

1.1 OVERVIEW

When it comes to collecting and evaluating biological data, biometrics is where the science and art meet. Biometrics is the study and use of human identifying traits for identification purposes via the measurement and analysis of biological variables such as DNA, fingerprints, eye retina and irises, voice pattern, face pattern, and measurements. Compared to the conventional and present methods, the biometric identification approach has several benefits that we encounter on a regular basis. Identifying and verifying information are the two primary functions. A typical contemporary automated teller machine (ATM) will include a central processing unit (CPU) to manage the user interface and transaction-related devices, a magnetic or chip card reader to verify the customer's identity, a PIN pad, and a secure crypto-processor, all housed in a protective casing.

A customer-facing display, a record printer to document their purchase, a secure location to keep sensitive machinery components (a vault), a visually appealing enclosure for sensors and indications, and a function key button complete the transaction. These days, a lot of individuals use ATMs. There are many pros and cons to the rapid expansion of the banking industry.

The primary goal of this system is the development of an embedded system for use in ATM security applications. Under this approach, customers will only be able to use ATMs if bank tellers have taken their fingerprints when they opened an account. These automated teller machines function by having the user's name shown on an LCD screen linked to the microcontroller as soon as

International Journal of Engineering Research and Science & Technology

https://doi.org/10.62643/ijerst.2024.v20.i3.pp232-237

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue 3, 2024

they press their finger on the fingerprint module. Users are unable to make purchases unless their accounts are originally activated using a fingerprint. These days, most people use ATMs, which stand for "Automatic Teller Machines," to exchange cash quickly and easily. But the number of cases of financial crimes has been on the increase recently; many thieves break into ATMs and illegally take customers' credit card details and passwords. Customers may suffer tremendous financial losses if criminals get access to their bank cards and quickly deplete their funds. The present financial cycle is centered on how to maintain a genuine client identity. The conventional way of authenticating users at ATMs, which often involves entering both a credit card number and a password, has its limitations. Verifying the client's identity with just their payment card and password is not foolproof. Combining the original password authentication method with biometric identification technology helps to better verify clients' identities and achieve the purpose of making ATM machines safer. The algorithm for fingerprint recognition has been continuously updated in recent years, which has given us new verification means.

II.EXISTING SYSTEM

For all of our financial needs, we rely on ATMs here in our nation. Customers of financial institutions can access their accounts and conduct a variety of financial transactions—including withdrawals, deposits, transfers, and information requests—through automated teller machines (ATMs) at any time and from any location, eliminating the need for human interaction. Most up-to-date automated teller machines (ATMs) require users to insert a plastic card (or other suitable payment method) before authenticating their identity. This authentication process involves entering a personal identification number (PIN), which must correspond with the PIN either stored on the card's chip (if it has one) or in the database of the issuing financial institution.

Customers may do a lot of different financial things, such check balance inquiries, cash withdrawals, and mobile phone credit, all via their deposit or credit accounts, which they can access at an ATM. You can use ATMs to get cash even while you're not in your own country. The bank will use its exchange rate to convert the funds if the currency being taken from the ATM is different from the currency that the bank account is denominated in.

III.PROPOSED SYSTEM

For all of our financial needs, we rely on ATMs here in our nation. Customers of financial institutions can access their accounts and conduct a variety of financial transactions—including withdrawals, deposits, transfers, and information requests—through automated teller machines (ATMs) at any time and from any location, eliminating the need for human interaction. Our suggested solution incorporates a fingerprint sensor that verifies the user's identity upon scanning their finger. a
It would seem that a biometric authentication system would be the perfect answer to authentication issues; nevertheless, there are several limitations to biometric authentication.
Biometrics is an emerging field of technology with several potential civilian applications; it is already seeing extensive usage in forensics applications like criminal identification and jail security. Automated teller machines (ATMs), mobile phones, smart cards, desktop computers, workstations, and computer networks may all benefit from biometric security. Keyless entry systems that use biometrics may replace traditional car keys.
The following are the two primary goals of this paper:
1. To include fingerprinting into the ATM system's access control mechanism.
2. Establishing a foundation for the ATM system that incorporates fingerprint verification.

IV.LITERATURE REVIEW

When it comes to software, system analysis is all about managing and documenting the many stages of the life cycle, including:

Each phase consists of the following: study, design, development, implementation, and testing.

An overview is provided at the outset of software analysis, followed by a more in-depth

International Journal of Engineering Research and Science & Technology
https://doi.org/10.62643/ijerst.2024.v20.i3.pp232-237
ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 3, 2024

examination. The analyst quickly assesses the requirements and determines whether the cost is beneficial during the preliminary analysis. The program is built and strengthened by detailed analysis, which investigates all the cornered elements in depth.

Program Requirement Specification (SRS) documents spell out exactly what the proposed program should be able to achieve without going into detail about the code itself.

Key Performance Indicators

1) There has to be a high throughput and a minimal operating time.
2) The results should be accurate and produced promptly.

V.MODULES

The fundamental working principles of the majority of biometric technology systems are universal. A user must first enroll in the biometric system in order to register.

1. Enrollment:

Enrollment refers to the steps used to obtain, access, process, and store a user's biometric data in a template format for future usage in a biometric system. Following enrollment, the template(s) created are used to undertake further verification and identification attempts.

2. Presentation:

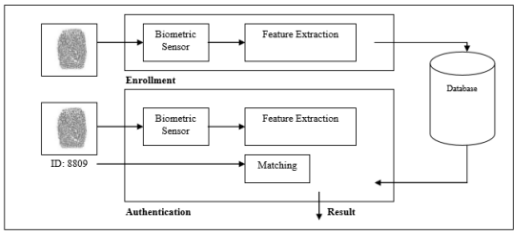
The user inputs their biometric information into an acquisition device, which is the hardware responsible for collecting biometric data, throughout the presentation process. In order to present oneself, one may need to gaze into a camera, put one's finger on a platen, or repeat a pass phrase; these steps vary per biometric system.

3. Biometric data:

The raw, unfiltered picture or recording of a person's biometric data that they provide. Biometric samples and raw biometric data are other names for the unprocessed data. You can't do biometric matching using raw biometric data. Instead, biometric templates are generated using user data supplied during registration and verification, and in almost all systems, this data is then destroyed. Thus Instead of storing biometric data, biometric systems utilize it to create templates. A unique identifier, such a username or ID, must be created in order to enroll. When entering personal information, the user or administrator often generates this identification. The user inputs the identification and then supplies biometric data upon returning to verify. After collecting biometric data, a feature extraction procedure may be used to produce biometric templates.

4. Feature extraction:

Extracting unique traits from biometric data and encoding them automatically to create a template is known as feature extraction. At the moment of registration or verification, or whenever a template is produced, feature extraction occurs. Image and data optimization and filtering are part of feature extraction to help find features more precisely. For instance, whereas voice-scan technologies often filter certain patterns and frequencies, fingerprint-scan technologies typically narrow the ridges in a fingerprint picture to the width of one pixel. The efficiency of a biometric system is highly dependent on the quality of its feature extraction, as this determines how well the system can create templates.



VI.OUTPUT

In order to improve security, we are using the user's fingerprint for authentication in our proposed online banking application instead of their PIN or password, which is the method used in all other banking programs. The modules below are what we created in order to carry out this project.

1) Sign-up: This module allows users to create an account and sign up for the application using their password, username, and finger print image. All registration information will be kept in a MySQL database.
2) Login: With this module, a user may access the program by providing their password, username, and the fingerprint picture they provided at registration to verify their identity.

International Journal of Engineering Research and Science & Technology

https://doi.org/10.62643/ijerst.2024.v20.i3.pp232-237

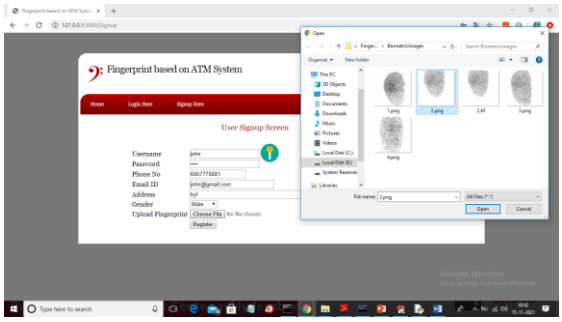
ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue 3, 2024

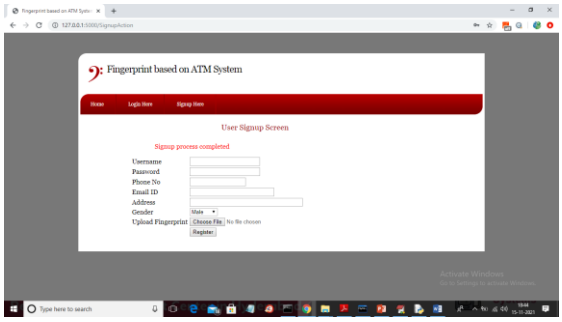
3) Deposit: Following successful authentication, the user may contribute money to his account by making a deposit.
4) Withdraw: If there is enough balance available, the user may use this to withdraw the desired amount.
5) examine Balance: The user can use this module to examine the available balance.

Copy the material from "DB.txt" to build a database in MySQL first, then paste it into MySQL.

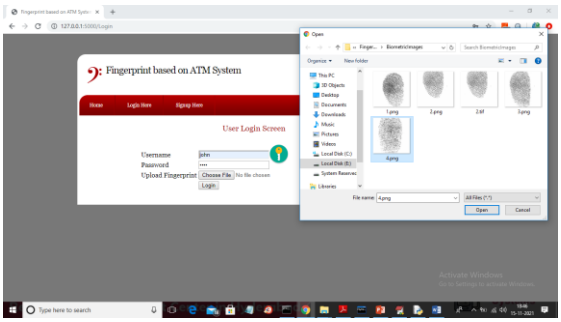
Double-clicking the "run.bat" file launches the Python FLASK server for the project.



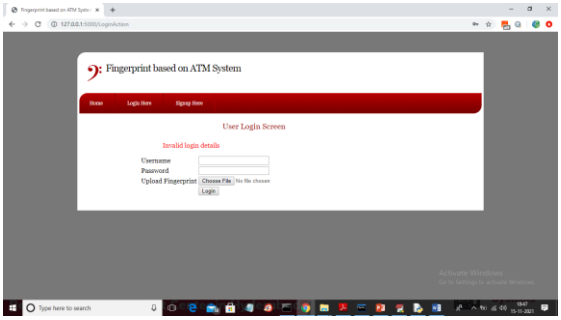
Complete the registration form on the top page, choose the finger print image, and click "Open" to load the picture and see the screen below.



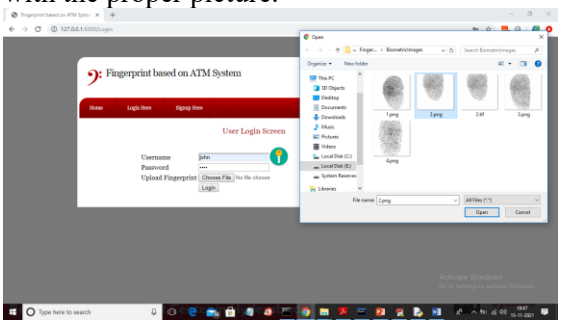
After clicking the "Register" button on the above page, we will get a message stating that the "Signup process completed." Click the "Login Here" link to see the screen below.



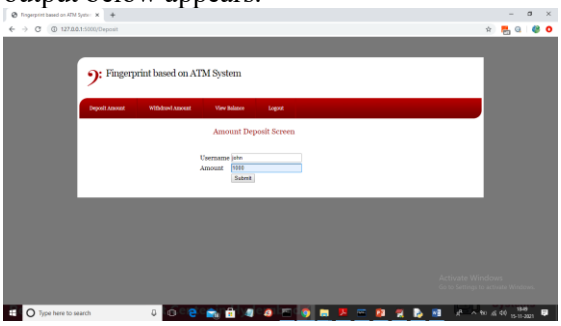
I'm logged in and have selected the incorrect finger print ('4.png') on the above page. Clicking the 'Open' button brings up the screen below.



Login failed on the screen above; try again with the proper picture.



I'm now uploading the right picture on the above page, and when I click "Login," the output below appears.



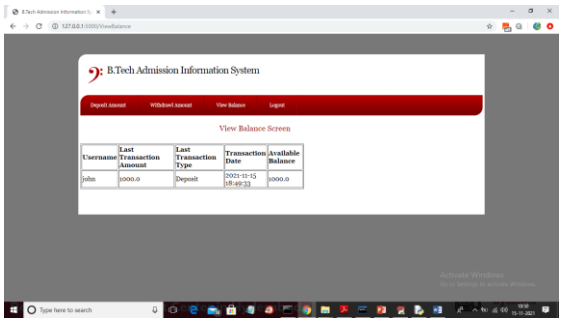
The username will automatically appear on the page above. Enter the desired amount and click "Submit" to finish the transaction, which will result in the output below.

International Journal of Engineering Research and Science & Technology

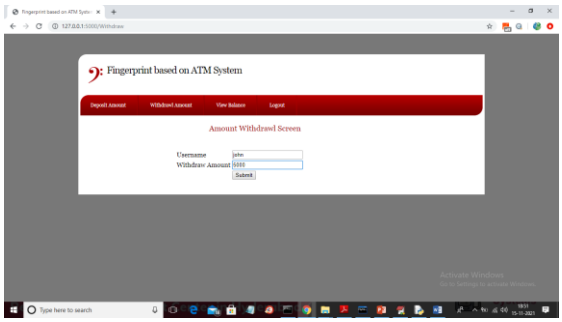
https://doi.org/10.62643/ijerst.2024.v20.i3.pp232-237

ISSN 2319-5991 www.ijerst.com

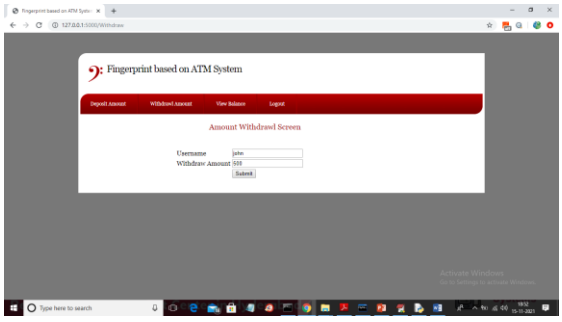
Vol. 20, Issue 3, 2024



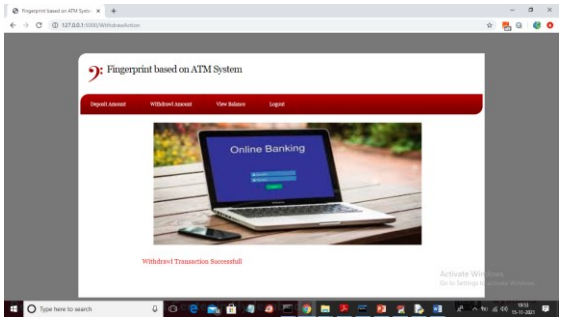
The deposit transaction is shown on the top page; click the "Withdrawl Amount" link to see the screen below.



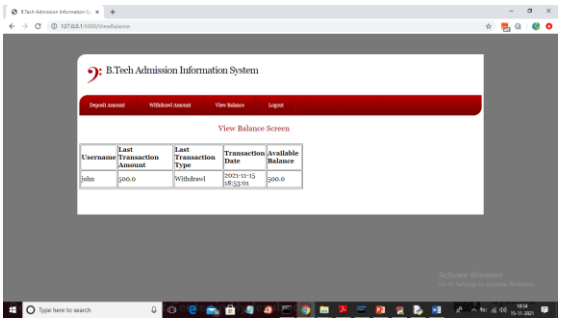
I'm withdrawing more money from the above screen than what's available to obtain the below screen.



500 is withdrawn in the above screen; click "Submit" to see the screen below.



Withdrawal transaction completed on the above page; verify balance once more.



Now, the available balance on the screen above is 500. In a similar manner, you may carry out N transactions.

VII.CONCLUSION

Autonomous systems are a big part of our daily lives in the contemporary world. One may clearly see where the number of ATM facilities is fast increasing, given the significant development in societal computerization and automation. The majority of people routinely use ATMs. A financial transaction, the simplicity of exchanging money, etc., are excellent examples. Thus, there is a crucial component known as security.

The consistency and dependability of owner identification led to significant improvements in the security features. Because fingerprint technology is the foundation of the whole system, it is dependable, user-friendly, and safer. As far as we are aware, fingerprints are the most widely used biometric for identity verification worldwide. Some governments across the globe continue to use fingerprint technology in forensic investigations to identify both criminals and their own people from crime scenes.

Numerous criminals tamper with the ATM terminal in order to obtain cardholder information illegally. Users' accounts are open to assault after their bank card is lost and their password is compromised. Conventional ATM systems often need a password or PIN in addition to a card—credit, debit, or smart—for authentication, which is undoubtedly flawed. There are a number of drawbacks to the current user authentication methods, which use identity cards and PINs (personal identification numbers) or passwords and user

https://doi.org/10.62643/ijerst.2024.v20.i3.pp232-237
ISSN 2319-5991 www.ijerst.com
Vol. 20, Issue 3, 2024

IDs (identifiers).

REFERENCES

[1] 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.

[2] Edmund Spinella, Biometric Scanning Technologies: Finger, Facial and Retinal Scanning, Available at:https://www.sans.org/readingroom/whitepapers/authenticati on/biometric-scanningtechnologies-finger-facial-retinal-scanning-1177.

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

[4] 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.

[5] 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/jcompeleceng.2020.106784

[6] 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

[7] 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.

[8] 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.

[9] LO Gorman Overview of Fingerprint Verification Technologies, Information Security Technical Report, Vol. 3, No. 1, p. 21-32, 1998.

[10] 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.