IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BANKING SYSTEM USING SECURED FINGERPRINTS

[1]G. Manoj Kumar, [2] Mutyala Pravallika, [1]Associate Professor, [2]MCA Final Semester, [1]Master of Computer Applications

[1]Sanketika Vidya Parishad Engineering College, Visakhapatnam, Andhra Pradesh, India.

Abstract: The main aim of this project to provide secure banking system, by taking fingerprints as authorized identity at ATM/banks. The purpose of the project is to provide a secured and reliable environment to the customers for their banking transactions by providinga unique identity to every user using the FINGER PRINT identification technology. 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 viaATM, 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. 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. There is no worry of losing ATM card and no need to carry ATM card in your wallet. You just have to use your fingerprint in order to do any banking transaction. The user has to login using his fingerprint and he has to enter the pin code in order to do further transaction. The user can withdraw money from his account. User can transfer money to various accounts by mentioning account number. In order to withdraw money user has to enter the amount he want to withdraw and has to mention from which account he want to withdraw. The user must have appropriate balance in his ATM account to do transaction. User can view the balance available in his respective account. The system will provide the user to view last 5 transactions.

I.INTRODUCTION

Biometrics is the art of science and technology of measuring and analyzing biological data. If biometrics refers to technologies that measure and analysis human body characteristics, such as DNA, fingerprinting, eye retina and irises, voice pattern, facial pattern and measurement for authentication purposes. Biometrics identifier method provides several advantages over the traditional method and current method used in our daily life. Basically concentrate on two function one is for identification and other verification. A modern ATM is typically made up of the devices like CPU to control the user interface and devices related to transaction, magnetic or chip card reader to identify the customer, Pin pad, secure crypto-processor generally within a secure cover. Display to be used by the customer for performing the transaction, function key button, record printer to provide the customer with a record of their transaction, to store the parts of the machinery requiring restricted access- vault, housing for aesthetics, sensors and indicators. In this modern era there are many people using ATM. Fast development of banking has various advantages and disadvantages. The main objective of this system is to develop an embedded system, which is used for ATM security applications. In these system, Bankers will collect the customer fingerprints while opening the accounts then customer will only access ATM machine. The working of these ATM machine is when

customer place finger on the finger print module it displays the name of the customer on the LCD connected to the micro controller. If the user does not have a account activated by a fingerprint initially it does not allow the user to do transactions. Nowadays, using the ATM (Automatic Teller Machine) which provides customers with the convenient banknote trading is very common. However, the financial crime case rises repeatedly in recent years; a lot of criminals' tamper with the ATM terminal and steal user's credit card and password by illegal means. Once user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring enormous financial losses to customer. How to carry on the valid identity to the customer becomes the focus in current financial circle. Traditional ATM systems authenticate generally by using credit card and the password, the method has some defects. Using credit card and password cannot verify the client's identity exactly. In recent years, the algorithm that the fingerprint recognition continuously updated, which has offered new verification means for us, the original password authentication method combined with the biometric identification technology verify the clients' identity better and achieve the purpose that use of ATM machines improve the safety effectively.

1.1 Existing System

We are using ATM's in our country for all our banking activities. An automated teller machine (ATM) is an electronic telecommunications device that enables customers of financial institutions to perform financial transactions, such as cash withdrawals, deposits, transfer funds, or obtaining account information, at any time and without the need for direct interaction with bank staff. On most modern ATMs, customers are identified by inserting a plastic ATM card (or some other acceptable payment card) into the ATM, with authentication being by the customer entering a personal identification number (PIN), which must match the PIN stored in the chip on the card (if the card is so equipped), or in the issuing financial institution's database. Using an ATM, customers can access their bank deposit or credit accounts in order to – make variety of financial transactions such as cash withdrawals, check balances, or credit mobile phones. ATMs can be used to withdraw cash in a foreign country. If the currency being withdrawn from the ATM is different from that in which the bank account is denominated, the money will be converted at the financial institution's exchange rate.

1.1.2 Challenges

Accuracy and False Acceptance/Rejection Rates**:**

- **False Rejection Rate (FRR)**: The system might incorrectly reject a legitimate user, causing inconvenience.
- **False Acceptance Rate (FAR)**: The system might incorrectly accept an unauthorized user, compromising security.

Data Privacy and Security: Storing biometric data requires stringent security measures. Breaches can expose sensitive biometric information, which, unlike passwords, cannot be changed if compromised.

Environmental Factors: Fingerprint scanners can be affected by environmental conditions such as dirt, moisture, and temperature, which may impact their performance.

Hardware and Software Limitations: High-quality scanners are expensive, and cheaper models might not provide adequate accuracy or durability.

User Variability: Fingerprint quality can vary due to age, injuries, or skin conditions. This variability can affect the system's effectiveness.

I**ntegration with Existing Systems**: Integrating fingerprint authentication with legacy banking systems can be complex and costly.

Regulatory and Compliance Issues: Different regions have varying regulations regarding the use and storage of biometric data. Ensuring compliance can be challenging.

Spoofing and Fraud: Advanced spoofing techniques can replicate fingerprints, posing a risk of unauthorized access.

User Acceptance and Adaptation: Users might be hesitant or uncomfortable with biometric systems, affecting adoption rates.

1.2 Proposed system:

We are using ATM's in our country for all our banking activities. An automated teller machine (ATM) is an electronic telecommunications device that enables customers of financial institutions to perform financial transactions, such as cash withdrawals, deposits, transfer funds or obtaining account information, at any time and without the need for direct interaction with bank staff. A biometric authentication system seems to be an excellent solution to authentication problems; however biometric authentication has some weaknesses. Biometrics is a rapidly evolving technology that is being widely used in forensics, such as criminal identification and prison security, and that has the potential to be used in a large range of civilian application areas. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. In automobiles, biometrics can replace keys with keyless entry devices.

There are two main objectives of this paper, as follows: -

- To integrate the fingerprinting in access control for ATM system.
- To purpose a framework for the ATM system using fingerprint verification.

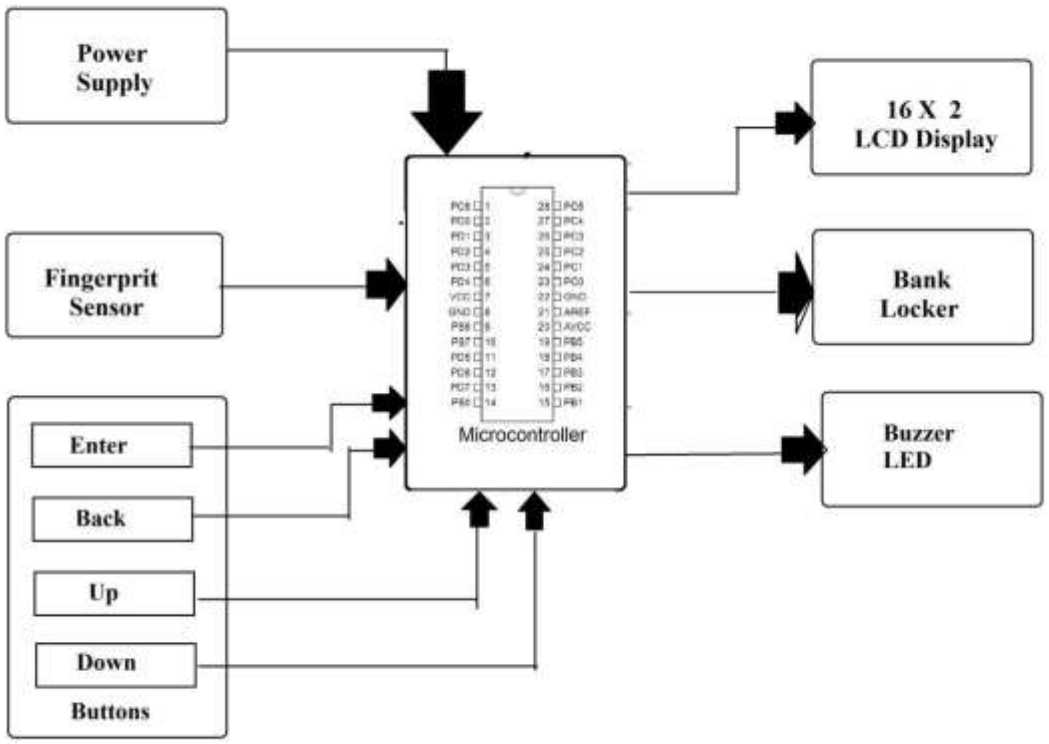

Fig 1: Work Flow

1.2.1 Advantages

Enhanced Security: **Fingerprints are unique to each individual, making it difficult for unauthorized users to gain access.**

Convenience: Fingerprint authentication is quick and easy compared to traditional methods like passwords

or PINs, reducing friction in the user experience.

Reduced Fraud Risk: Since fingerprints are hard to replicate or steal, the risk of fraud is lower compared to traditional authentication methods.

No Need for Physical Tokens: Unlike smart cards or tokens, fingerprints are always available and do not require carrying extra devices.

Efficient User Verification: Biometrics provide rapid verification, speeding up processes like account login or transaction approvals.

Enhanced Accountability: Biometric data can help ensure that only authorized individuals perform transactions, providing a clear audit trail.

Improved Access Control: Fingerprint systems can be integrated with other security measures, such as multi-factor authentication, to provide layered security.

Reduced Password Fatigue: Users do not need to remember or change passwords, reducing the risk of password-related issues.

Personalization: Fingerprint systems can be customized for individual preferences and security levels, offering a more tailored user experience.

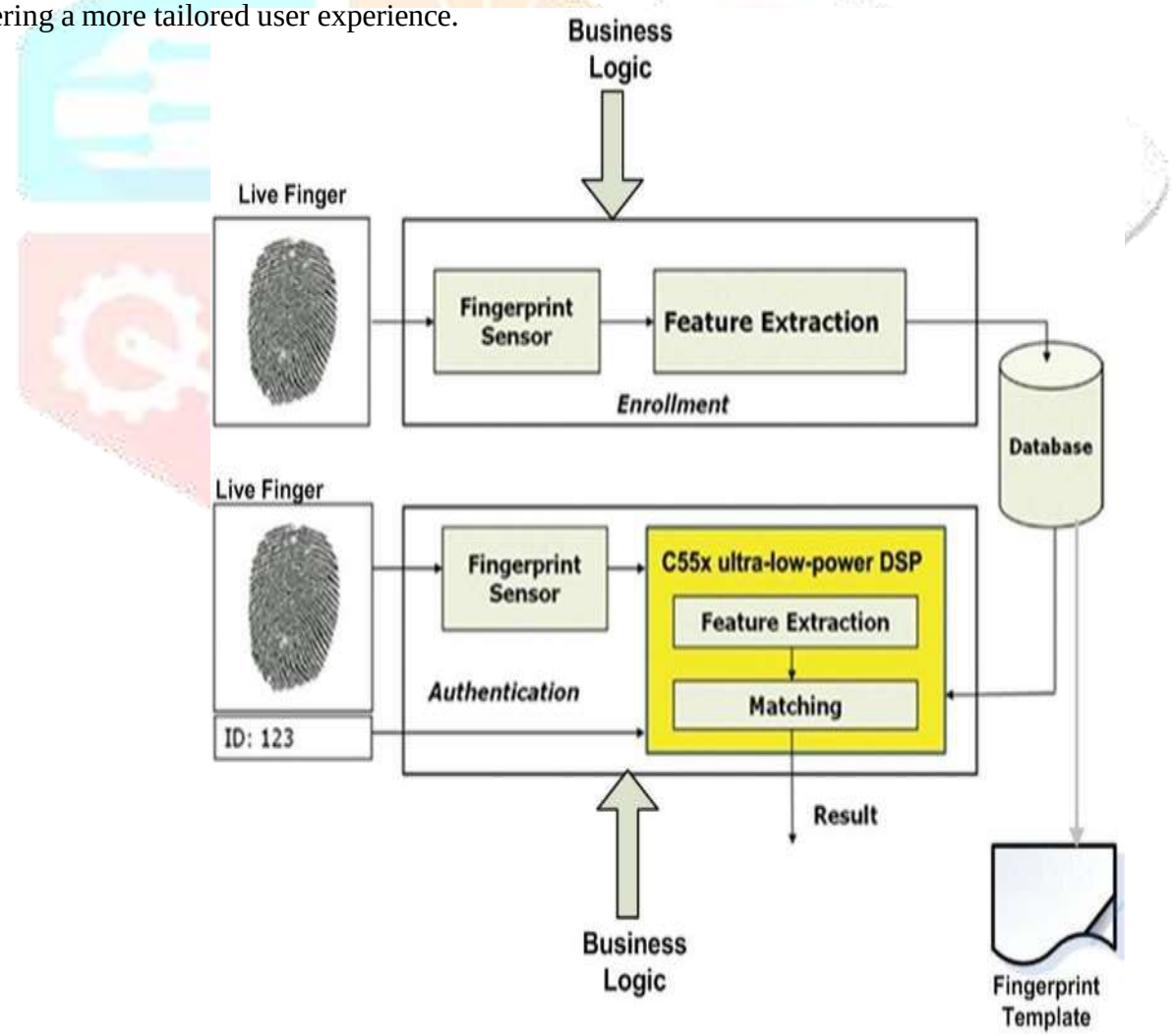

Fig – 2

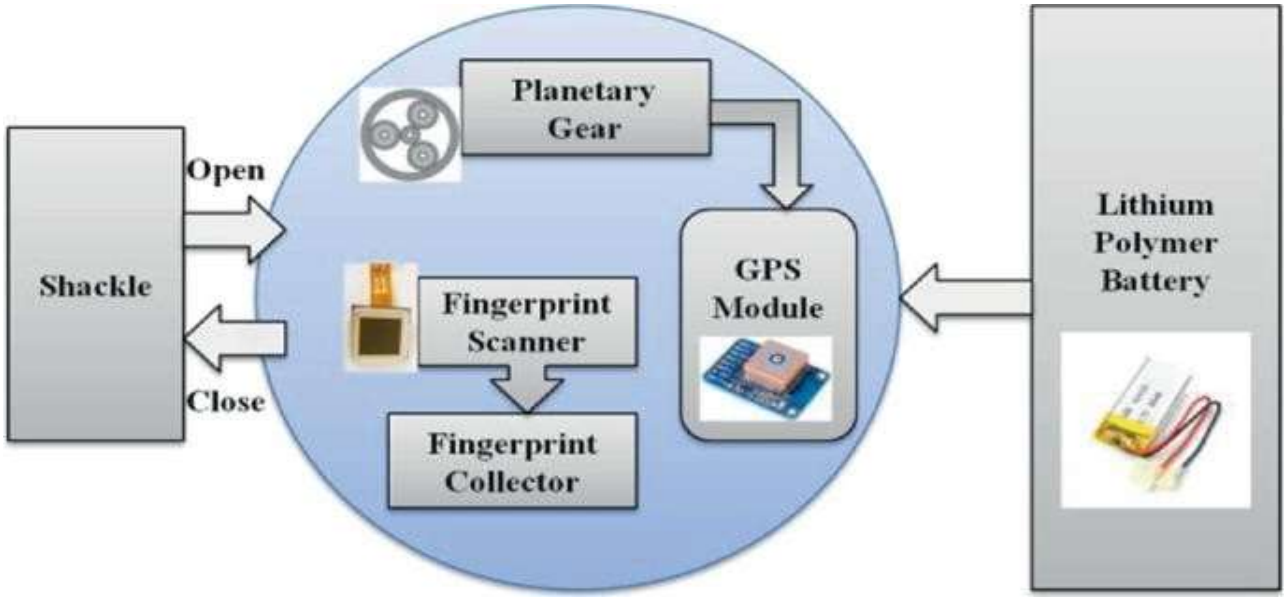

Fig - 3

II LITERATURE REVIEW

A literature review on secured banking systems using fingerprints involves examining existing research, technological advancements, challenges, and solutions in the field. Here's a structured overview of key areas to cover:

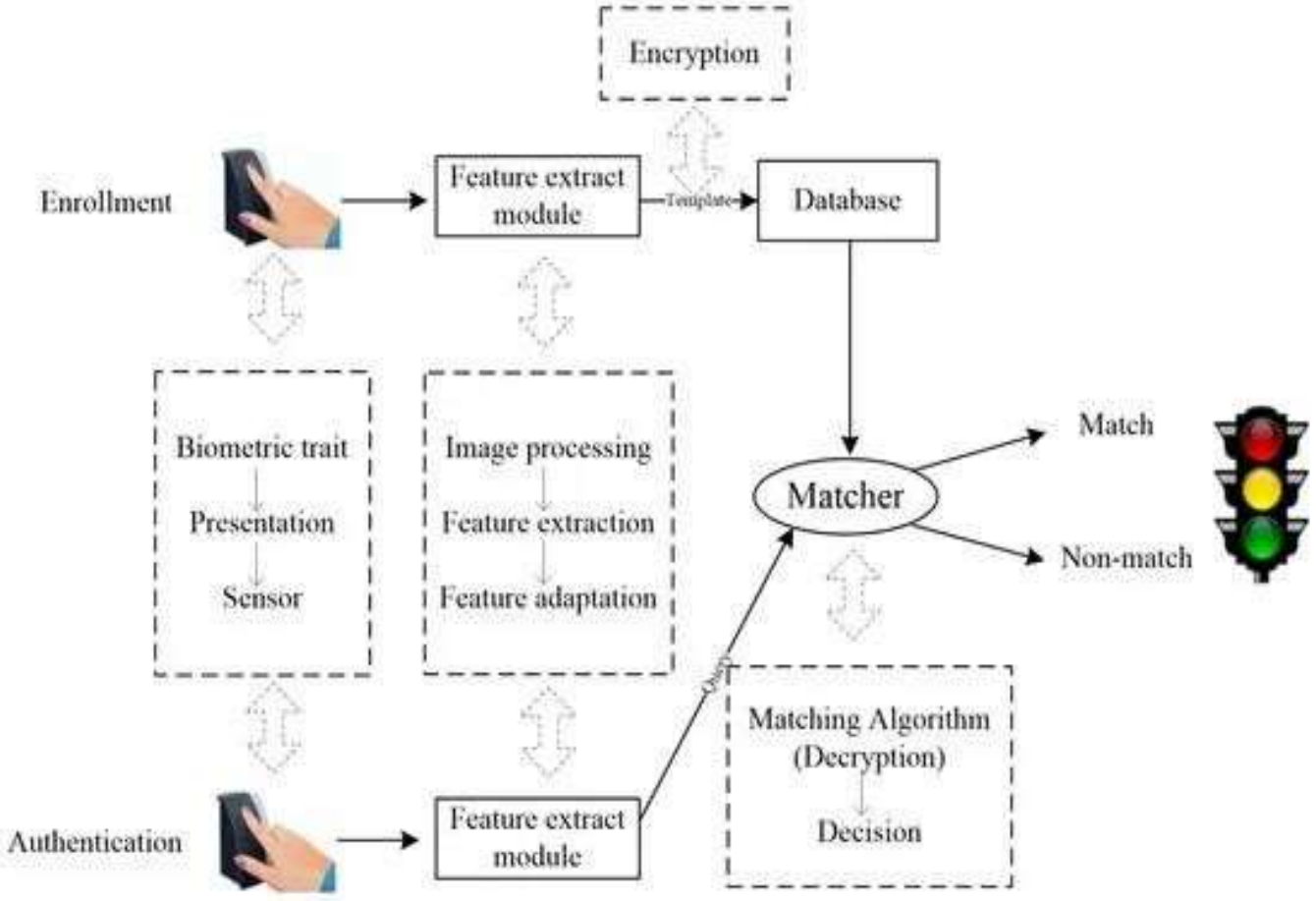

Fig - 4

1. Introduction to Biometric Authentication

- **Overview of Biometric Systems**: Introduction to different types of biometric systems (fingerprints, facial recognition, iris scans, etc.) with a focus on fingerprint technology.
- **History and Evolution**: Historical development of fingerprint recognition technology and its application in various security domains.

2. Fingerprint Recognition Technology

- **Fingerprint Acquisition**: Methods of capturing fingerprint images (optical, capacitive, ultrasonic).
- **Feature Extraction and Matching**: Algorithms used for feature extraction (e.g., minutiae-based, ridge-based) and matching techniques.
- **Accuracy and Performance Metrics**: Evaluation of performance metrics such as False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER).

3. Applications in Banking Systems

- **Case Studies**: Examination of case studies where fingerprint authentication has been implemented in banking systems.
- **Implementation Strategies**: Methods and best practices for integrating fingerprint authentication into existing banking infrastructures.
- **User Experience**: Studies on how fingerprint systems impact customer satisfaction and ease of use.

4. Security and Privacy Concerns

- **Data Security**: Analysis of how biometric data is stored and protected, and potential vulnerabilities.
- **Spoofing and Attacks**: Types of spoofing attacks (e.g., using fake fingerprints) and countermeasures.
- **Regulatory Compliance**: Overview of legal and regulatory requirements for handling biometric data (e.g., GDPR, CCPA).

5. Challenges and Limitations

- **Accuracy Issues**: Problems related to false acceptance/rejection rates and methods to improve accuracy.
- **User Variability**: Challenges related to user variability such as aging, skin conditions, and injuries.

6. Advancements and Future Directions

- **Technological Innovations**: Latest advancements in fingerprint recognition technology (e.g., 3D fingerprint scanners, multispectral imaging).
- **Integration with Other Systems**: How fingerprint authentication can be combined with other security measures (e.g., multi- factor authentication).

III METHODOLOGY MODULES

Most biometric technology systems use the same basic principles of operation. First, a person must be registered, or enrolled, on the biometric system.

Enrolment: The process by which a user's biometric data is initially acquired, accessed, processed, and stored in the form of a template for ongoing use in a biometric system is called enrolment. Subsequent verification and identification attempts are conducted against the template(s) generated during enrolment.

Biometric data: The biometric data users provide in an unprocessed image or recording of a characteristic.

The unprocessed data is also referred to as raw biometric data or as a biometric sample. Raw biometric data cannot be used to perform biometric matches. Instead, biometric data provided by the user during enrolment and verification is used to generate biometric templates, and in almost every system is discarded thereafter. Thus, Biometric systems do not store biometric data-systems use data for template creation. Enrolment requires the creation of an identifier such as a username or ID. This identifier is normally generated by the user or administrator during entry of personal data. When the user returns to verify, he or she enters the identifier, and then provides biometric data. Once biometric data has been acquired, biometric templates can be created by a process of feature extraction.

Feature extraction: The automated process of locating and encoding distinctive characteristics from biometric data in order to generate a template as called feature extraction. Feature extraction takes place during enrollment and verification-any time a template is created. The feature extraction process includes filtering and optimization of images and data in order to accurately locate features. For example, voice-scan technologies generally filter certain frequencies and patterns, and finger-scan technologies often thin ridges present in a fingerprint image to the width of a single pixel. Since quality of feature extraction directly affects a system's ability to generate templates, it is extremely important to the performance of a biometric system.

Fig - 5

3.1 Input

In a secured banking system using fingerprints, the primary inputs encompass several critical elements essential for the effective operation of the authentication process. Initially, biometric data acquisition involves capturing high-quality fingerprint images through various scanners, such as optical or capacitive devices. During the enrolment phase, users provide initial fingerprint samples that are used to create reference templates for future comparisons. Alongside biometric data, personal identification details like names, addresses, and account numbers are linked with the fingerprint data to facilitate user verification. The system also requires configuration inputs, including threshold settings for similarity levels and security policies governing biometric data handling, such as encryption and access controls. Environmental factors, such as temperature and humidity, can impact the performance of fingerprint scanners, necessitating calibration settings to maintain accuracy. Processing inputs involve feature extraction algorithms that analyse fingerprint images to identify distinctive characteristics and matching algorithms that compare these features with stored templates to verify identities. To ensure data protection, encryption keys and access control lists are utilized to secure biometric data and regulate access. Additionally, diagnostic data and user feedback are vital for system maintenance and improvement, helping to address any performance issues and enhance user experience. Compliance with regulatory and privacy standards is also crucial, involving documentation and procedures to safeguard biometric data in line with legal requirements.

3.2 Output

In a secured banking system using fingerprints, the output primarily consists of the results generated from the biometric authentication process. When a user attempts to access their account or perform transactions, the system processes their fingerprint input by comparing it against stored reference templates. The immediate output is a verification result, indicating whether the fingerprint matches a registered user or not. This result determines whether the user gains access or if further authentication steps are required. Additionally, the system generates logs of authentication attempts, including details such as timestamps, user IDs, and access outcomes, which are crucial for auditing and security monitoring. In cases where the fingerprint matches, the system may provide feedback to the user, such as a confirmation message or transaction authorization. Conversely, if the fingerprint does not match, the system outputs an error message or prompts for additional authentication measures. Outputs also include encrypted biometric data and configuration settings, which are used to update or maintain the system's performance. Overall, the outputs from a fingerprint-secured banking system are essential for ensuring accurate, secure, and efficient user authentication and transaction processing.

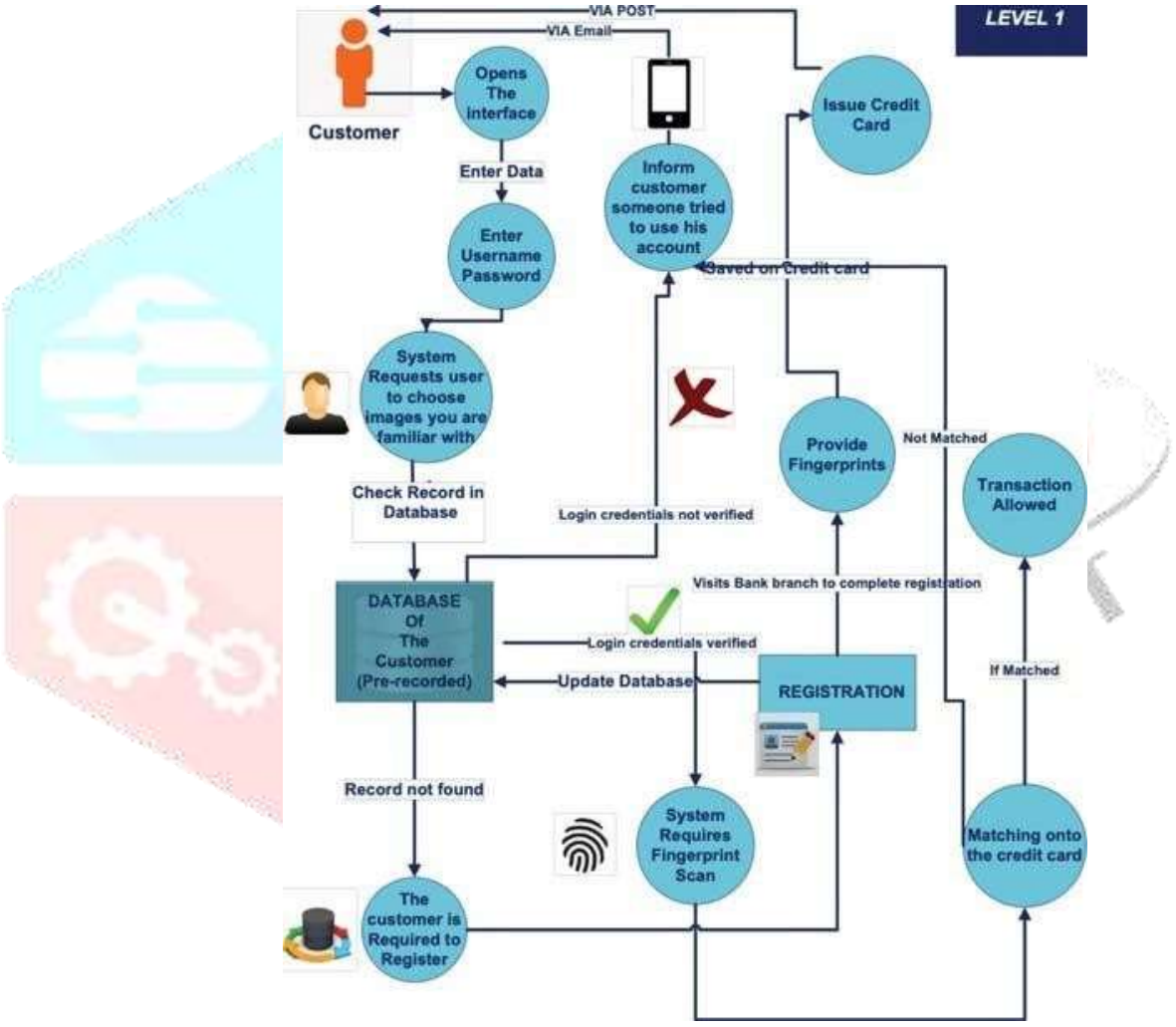

Fig - 6

IV RESULTS

The results of a secured banking system using fingerprints typically reflect the effectiveness and reliability of the authentication process. When a user's fingerprint is compared to stored reference templates, the primary result is a verification outcome indicating whether the fingerprint matches an authorized user. If the match is successful, the system grants access to the user's account or approves a transaction, providing a seamless and secure experience. Conversely, a failed match results in an authentication error or a request for additional verification steps, such as a password or another form of multi-factor authentication. Additionally, the system produces detailed logs of each authentication attempt, including timestamps and

user IDs, which are crucial for monitoring and auditing purposes. The accuracy of the system is assessed through metrics like False Acceptance Rate (FAR) and False Rejection Rate (FRR), with lower rates indicating higher performance and security. Overall, the results reflect how well the fingerprint system performs in terms of user accessibility, security, and operational efficiency, ensuring that only authorized individuals can access sensitive banking services while maintaining robust protection against unauthorized access.

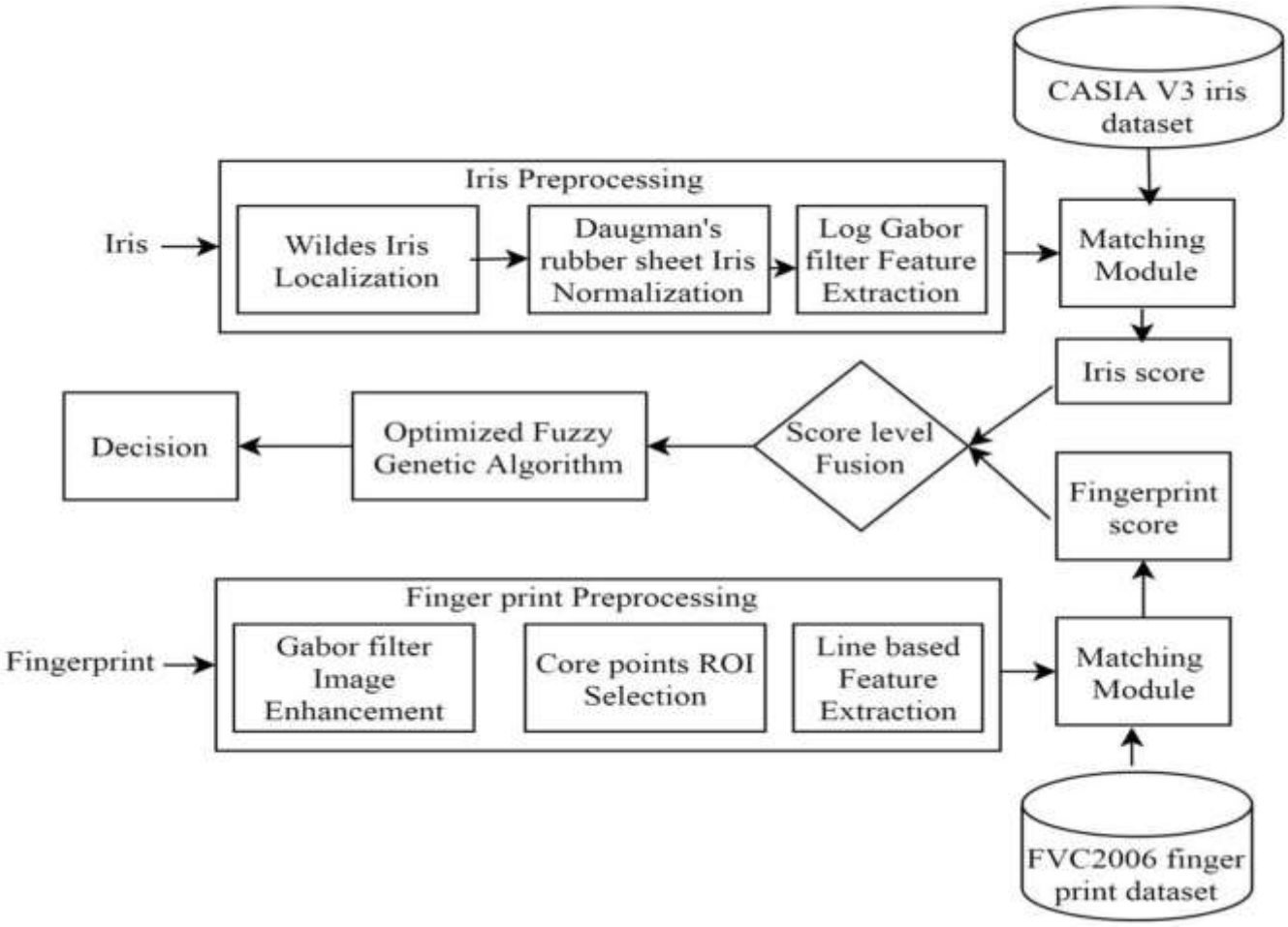

Fig - 7

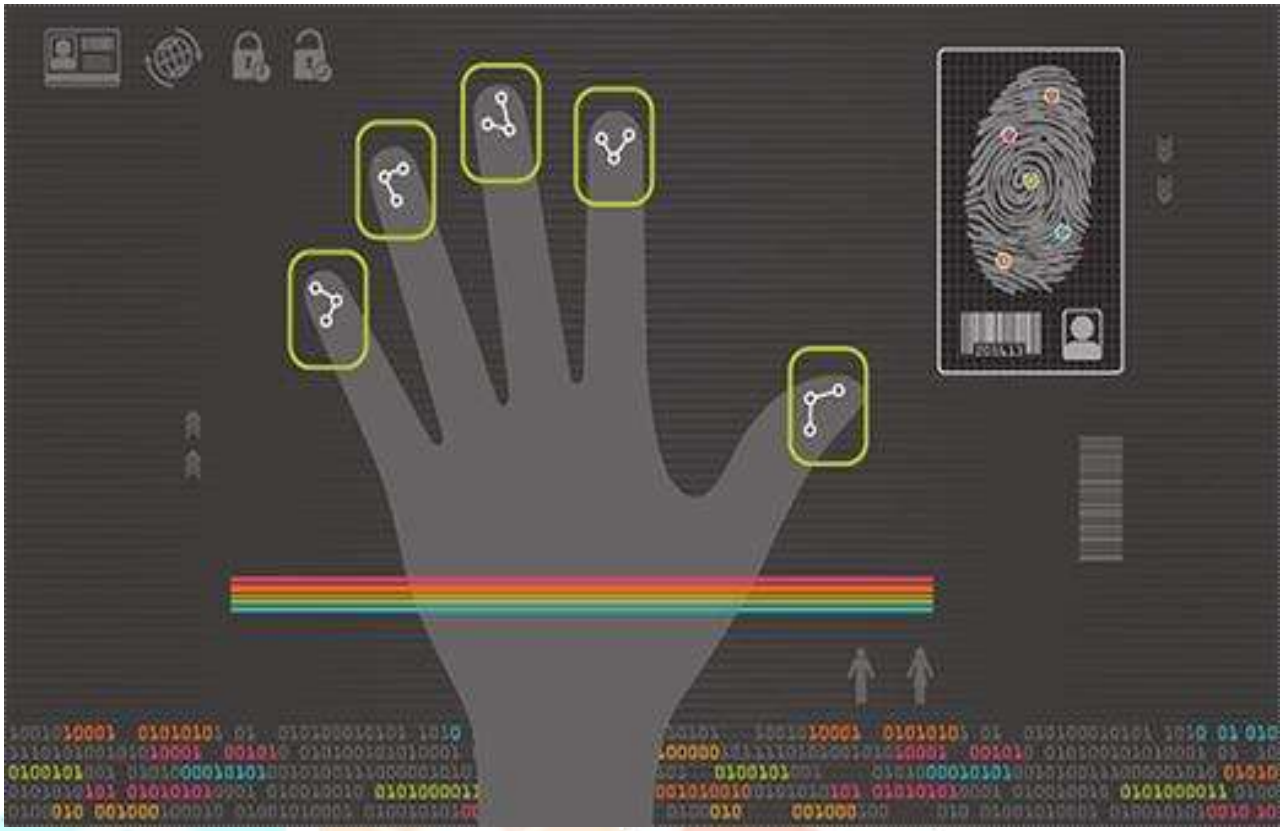

Fig - 8

V DISCUSSION

Secured banking system using fingerprints involves evaluating various aspects of this technology, including its effectiveness, advantages, challenges, and potential improvements. Here's an overview:

Effectiveness and Benefits

1. **Enhanced Security**: Fingerprint authentication provides a high level of security due to the uniqueness of each individual's fingerprints. This biometric method is generally more secure than traditional password-based systems, which are vulnerable to theft and hacking.
2. **Convenience**: The use of fingerprints streamlines the authentication process. Unlike passwords or PINs, which users might forget or need to update, fingerprints are always available and require minimal effort to use. This improves the user experience and speeds up transaction processing.
3. **Fraud Reduction**: The difficulty of replicating fingerprints significantly reduces the risk of fraud. Since fingerprints are unique and hard to forge, unauthorized access becomes considerably more challenging.
4. **Operational Efficiency**: Fingerprint systems can enhance operational efficiency by automating identity verification processes, reducing the need for manual intervention and lowering administrative costs associated with managing and resetting passwords.

Challenges

1. **Accuracy and Reliability**: While fingerprint systems are generally accurate, they are not infallible. Issues such as false acceptance (allowing unauthorized access) and false rejection (denying access to authorized users) can occur, particularly with low-quality scanners or challenging environmental conditions.
2. **Privacy Concerns**: The collection and storage of biometric data raise significant privacy issues. Unlike passwords, biometric data cannot be changed if compromised. Ensuring robust data protection and compliance with privacy regulations (e.g., GDPR) is critical.
3. **Environmental and Physical Factors**: Factors such as dirt, moisture, and skin conditions can

affect the performance of fingerprint scanners. This can lead to difficulties in capturing clear fingerprint images, potentially impacting system accuracy.

4. **Spoofing and Security Risks**: Advanced spoofing techniques, such as using fake fingerprints, can pose security risks. Implementing anti-spoofing measures and using advanced scanning technologies can help mitigate these risks.
5. **Integration and Cost**: Integrating fingerprint authentication with existing banking systems can be complex and costly. The initial investment in high-quality fingerprint scanners and the integration with legacy systems can be significant.

Potential Improvements

1. **Technological Advancements**: Ongoing advancements in fingerprint technology, such as 3D scanning and multispectral imaging, can improve accuracy and reliability. These technologies can capture more detailed fingerprint data and perform better under various conditions.
2. **Multi-Factor Authentication**: Combining fingerprint authentication with other security measures, such as passwords or smart cards, can enhance overall security by providing multi-factor authentication.
3. **Enhanced Anti-Spoofing Measures**: Implementing sophisticated anti-spoofing techniques, such as liveliness detection and advanced pattern recognition, can help prevent unauthorized access attempts using fake fingerprints.
4. **User Education and Training**: Educating users about proper fingerprint enrollment and usage practices can help minimize issues related to fingerprint quality and improve system performance.

VI CONCLUSION

The implementation of a secured banking system using fingerprints demonstrates a significant advancement in authentication technology, providing a blend of enhanced security, user convenience, and operational efficiency. Fingerprint authentication effectively mitigates the risks associated with traditional methods like passwords, offering a high level of protection against unauthorized access and fraud due to the uniqueness of each individual's fingerprints. It simplifies the user experience by eliminating the need for password management and speeds up the authentication process. However, challenges such as accuracy issues, privacy concerns, environmental factors, and potential spoofing risks must be addressed. Ensuring robust data protection, incorporating advanced scanning technologies, and implementing anti-spoofing measures are crucial for maximizing the benefits of fingerprint authentication. Overall, while fingerprint systems present a promising solution for secure banking, ongoing improvements and careful management of associated risks are essential for maintaining system effectiveness and user trust.

VII FUTURE SCOPE

The future scope of secured banking systems using fingerprints holds promising potential as technology continues to evolve and integrate with emerging innovations. Advancements in fingerprint recognition technology, such as high-resolution 3D imaging and multispectral scanners, are expected to significantly enhance accuracy and reliability, even in challenging conditions. The integration of artificial intelligence and machine learning can further improve the system's ability to distinguish between genuine and spoofed fingerprints, thereby increasing security. Additionally, combining fingerprint authentication with other biometric modalities, like facial recognition or voice verification, could lead to more robust multi-factor authentication systems, offering layered security that addresses various vulnerabilities. The continued development of privacy-preserving technologies and compliance with stringent regulatory standards will be crucial for maintaining user trust and protecting sensitive biometric data. As digital banking evolves, the adoption of fingerprint-based systems will likely expand, offering more seamless and secure user experiences while driving innovations in biometric technology and cybersecurity.

VIII ACKNOWLEDGEMENT

G Manoj Kumar working as an Assistant Professor in Master of Computer Applications (MCA) in Sanketika Vidya Parishad Engineering College, Visakhapatnam completed his post-graduation in Andhra University College of Engineering (AUCE). With accredited by NAAC with his areas of interest in Python, Database Management System, PSQT, FLAT.

Mutyala Pravallika is studying her 2nd year of Master of Computer Applications in Sanketika Vidya Parishad Engineering College, affiliated to Andhra University, accredited by NAAC. With her interest in machine learning method and as a part of academic project, she used Secured Banking System Using Fingerprints a result of privacy protection, and providing more secure to the users. This was completely developed project. Along with code has been submitted for Andhra University as an Academic Project. In completion of her MCA.

REFERENCES

[1] Jain, A.K.; Flynn, P.; Ross, A.A. Handbook of Biometrics; Springer: New York, NY, USA, 2007.

[2] Riaz, N.; Riaz, N.; Riaz, A.; Riaz, A.; Khan, S.A.; Khan, S.A. Biometric template security: An overview. Sensor Rev. **2017**, 38, 120–127.

[3] Prabhakar, S.; Pankanti, S.; Jain, A.K. Biometric recognition: Security and privacy concerns. IEEE Secur. Priv. **2003**, 1, 33–42.

[4] Awad, A.I.; Hassanien, A.E. Impact of Some Biometric Modalities on Forensic Science. In Computational Intelligence in Digital Forensics: Forensic Investigation and Applications; Springer: Berlin, Germany, 2014; pp. 47–62.

[5] Zheng, G.; Shankaran, R.; Orgun, M.A.; Qiao, L.; Saleem, K. Ideas and challenges for securing wireless implantable medical devices: A review. IEEE Sens. J. **2016**, 17, 562–576.

[6] Zheng, G.; Fang, G.; Shankaran, R.; Orgun, M.A.; Zhou, J.; Qiao, L.; Saleem, K. Multiple ECG fiducial points- based random binary sequence generation for securing wireless body area networks. IEEE J. Biomed. Health Inf. **2017**, 21, 655–663

[7] Zheng, G.; Fang, G.; Shankaran, R.; Orgun, M.A. Encryption for implantable medical devices using modified one- time pads. IEEE Access **2015**, 3, 825–836.

[8] Awad, A.I.; Hassanien, A.E.; Zawbaa, H.M. A Cattle Identification Approach Using Live Captured Muzzle Print Images. In Advances in Security of Information and Communication Networks; Springer: Berlin, Germany, 2013;
pp. 143–152.

[9] The FBI Now Has the Largest Biometric Database in the World. Will It Lead to More Surveillance? Available

[10] U.S. Security Officials Will Begin Scanning All 10 Fingerprints of Most Non-Americans Traveling to the United States.

[11] Australia Wants to Streamline Its Border Control Using Biometrics. Available

[12] How Biometrics on Smartphones is Changing our Lives. Available

[13] MasterCard Trials Biometric Bankcard with Embedded Fingerprint Reader. Available

[14] Maio, D.; Maltoni, D.; Capelli, R.; Franco, A.; Ferrara, M.; Turroni, F. FVC-ongoing: On-Line Evaluation of Fingerprint Recognition Algorithms. 2013. Available

[15] Jain, A.K.; Ross, A.; Prabhakar, S. An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol. **2004**, 14, 4–20.

[16] Tipton, S.J.; White, D.J., II; Sershon, C.; Choi, Y.B. iOS security and privacy: Authentication methods, permissions, and potential pitfalls with touch id. Int. J. Comput. Inf. Technol. **2014**, 3, 482–489

[17] Ratha, N.K.; Connell, J.H.; Bolle, R.M. An analysis of minutiae matching strength. In Proceedings of the 3rd International Conference on Audio-and Video-Based Biometric Person Authentication, Halmstad, Sweden, 6–8 June 2001; pp. 223–228

[18] Jain, A.K.; Nandakumar, K.; Nagar, A. Biometric template security. EURASIP J. Adv. Signal Process. **2008**, 2008, 1–17

[19] El-Abed, M.; Lacharme, P.; Rosenberger, C. Privacy and Security Assessment of Biometric Systems; Cambridge Scholar Publishing: Cambridge, UK, 2015.

[20] Kang, H.; Lee, B.; Kim, H.; Shin, D.; Kim, J. A study on performance evaluation of the liveness detection for various fingerprint sensor modules. In Proceedings of the International Conference on Knowledge-Based and Intelligent Information and Engineering Systems, Oxford, UK, 3–5 September 2003; pp. 1245–1253.

[21] Schuckers, S.A. Spoofing and anti-spoofing measures. Inf. Secur. Tech. Rep. **2002**, 7, 56–62.

[22] Yang, W.; Hu, J.; Fernandes, C.; Sivaraman, V.; Wu, Q. Vulnerability analysis of iPhone 6. In Proceedings of the 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, New Zealand, 12–14 December 2016;
pp. 457–463.

[23] Tan, B.; Schuckers, S. Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing. In Proceedings of the Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06), New York, NY, USA, 17–22 June 2006; p. 26.
[24] Coli, P.; Marcialis, G.L.; Roli, F. Fingerprint silicon replicas: Static and dynamic features for vitality detection
`using an optical capture device. Int. J. Image Graphics **2008**, 8, 495–512.