Fingerprint and Iris Biometric Controlled Smart Banking Machine Embedded with GSM Technology for OTP

V.N. Sireesha, Assistant Professor, Department of ECE, Satya Institute of Technology and Management, Vizianagaram, Andhra Pradesh, India. Email: -sireesha.vn@sitam.co.in

Attada Manasa, B Tech Student, Department of ECE, Satya Institute of Technology and Management, Vizianagaram, Andhra Pradesh, India. Email: -attadamanasa29@gmail.com

Muddada Anusha, B Tech Student, Department of ECE, Satya Institute of Technology and Management, Vizianagaram, Andhra Pradesh, India. Email: -muddadaanusha27@gmail.com

Landa Usha Ramya, B Tech Student, Department of ECE, Satya Institute of Technology and Management, Vizianagaram, Andhra Pradesh, India. Email: - Ushalanda428@gmail.com

Pinninti Janardhan Rao, B Tech Student, Department of ECE, Satya Institute of Technology and Management, Vizianagaram, Andhra Pradesh, India. Email: -pinnintijana871@gmail.com

Arikathota Dhatri, B Tech Student, Department of ECE, Satya Institute of Technology and Management, Vizianagaram, Andhra Pradesh, India. Email: - dhatriarikathota@gmail.com

Jagarana Satyanarayana, B Tech Student, Department of ECE, Satya Institute of Technology and Management, Vizianagaram, Andhra Pradesh, India. Email: -jagaranasatya@gmail.com

ABSTRACT

This project aims to develop a highly secure and user-friendly smart banking machine that integrates fingerprint and iris biometric authentication with GSM technology for OTP (One-Time Password) verification. The system eliminates the need for traditional ATM cards and PINs, replacing them with advanced biometric authentication techniques to enhance security and convenience. The GSM module ensures secure OTP delivery to registered mobile numbers, providing an additional security layer for transactions.

Biometrics technology is rapidly progressing and offers attractive opportunities and inventions. In recent years, biometric identification has grown in popularity as a way of private identification in ATM authentication systems. Biometric authentication system is reliable, economical, save time, and has more advantage compare to other like visa cards.

The user suspects their password may be stolen or attack by thief then the user changes their password when they expect the password attack by the thief. In order to solve this kind of problem we design biometric authentication system, because biometrics is the science of using human measurements to identify people.

Biometric is selective because it has unique characteristics that is no one shares and remain the same over time. In this project, a microcontroller-based prototype of ATM cashbox access system using fingerprint sensor and Iris recognition module is implemented. An Arduino microcontroller developed by Microchip Technology is used in the system. This research, which can increase the speed of money withdrawal almost 3 times fast; could have positive impact on the customer's satisfaction.

Digital security has acquired special importance thanks to vast amount of digital information and therefore the high value that's frequently been attached thereto. Normally we use passwords for security. Effective user authentication applications are crucial to guard information security. In response to the growing number of threats to data security, a good sort of authentication mechanisms is developed. Here we introduce a new security system which uses finger iris recognition system for authentication in ATM networks.

***Keywords*:** Biometric security, biometric technology, ATM (Automated Teller Machine), Red-tacton, Point of Sale (POS).

I INTRODUCTION:

In recent years, interest in various biometric identification systems among computer system users has significantly increased. The applications of identification technologies are not limited to a single domain—they span across both government and private sectors. Fingerprint recognition, in particular, has attracted attention due to its potential to enhance the security of confidential and sensitive information.

Organizations in the field of information technology are also showing strong interest in biometric technologies such as fingerprint, facial, voice, and iris recognition to prevent unauthorized access to their networks. Payment processing, long considered the weakest link in online transactions, remains a primary concern despite advancements in e-commerce technologies. Fraud continues to rise annually, prompting financial institutions to explore innovative solutions to improve transaction security.

Among emerging solutions, biometric payment technology has gained significant traction as a promising approach to reduce fraud and identity theft. The effectiveness of iris recognition systems, however, heavily depends on accurate segmentation [1].

To address growing concerns over customer fund safety and the vulnerability of Personal Identification Numbers (PINs), the Central Bank of Nigeria (CBN) announced plans to implement biometric authentication for Point of Sale (PoS) terminals and Automated Teller Machines (ATMs) by 2015 [2]. This initiative followed earlier efforts by the bank to enhance consumer confidence, such as mandating the migration from magnetic stripe debit cards to EMV-compliant chip and PIN cards.

Many of the current issues in digital security stem from flaws in existing systems. As the amount and value of digital information continue to grow, ensuring its protection has become increasingly critical. While passwords remain a common method of authentication, their limitations have led to the development of more effective security measures.

In response to the rising threats to data security,

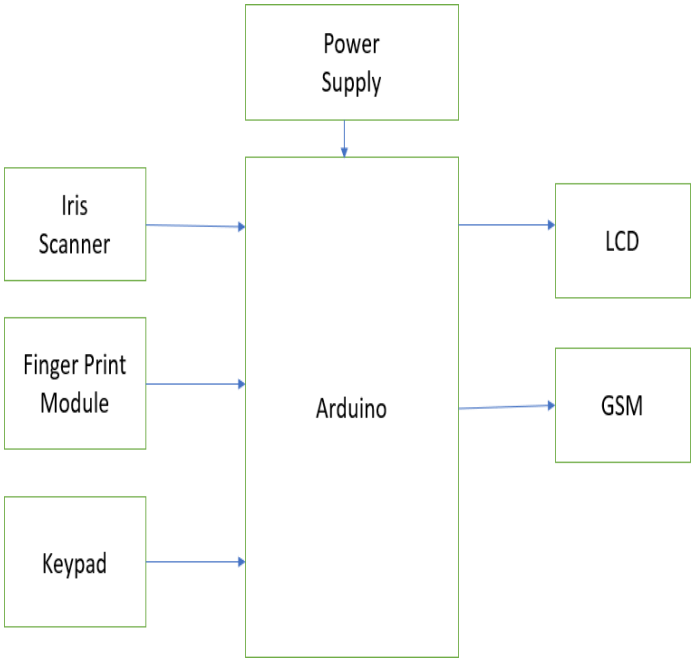

Fig 1 Proposed Block Diagram

a wide range of authentication mechanisms has been introduced. In this context, we propose a novel security system that utilizes a combined fingerprint and iris recognition approach for ATM network authentication.

II THEORIES PROPOSED

In the proposed model, ATM transactions are conducted without the use of a traditional ATM card. To enhance security, iris recognition is employed as a primary biometric identifier due to its reliability and convenience. The iris pattern is unique to each individual and can only be captured from a living person, making it a strong and tamper-resistant form of authentication.

For a transaction to be approved, both the iris and fingerprint of the user must successfully match the stored biometric data. If either of the biometric inputs fails to authenticate, the system automatically denies access by locking the ATM door. Additionally, an emergency alert is immediately sent to both the police and the registered customer via SMS, ensuring a swift response to any unauthorized access attempt.

2.1 Hardware Requirements

- Microcontroller
- Alarm System
- GSM Module
- Serial Communication Interface
- Electric Motor (for ATM door control)
- Fingerprint Sensor
- Iris Scanner

III Block Diagram:

The analysis phase is a crucial step in the development of any system. It involves a detailed examination of the system's requirements, functionalities, and constraints. In the context of a fingerprint and iris biometric controlled smart banking machine embedded with GSM technology for OTP, the analysis phase will focus on understanding the needs of the users, the technical requirements of the system, and the overall feasibility of the project. This phase will begin with a thorough review of the literature survey, identifying the limitations of existing systems and the potential benefits of the proposed system. The analysis will specific requirements of the system, including user requirements, software requirements, and hardware requirements. This will involve gathering information from various stakeholders, including potential users, banking professionals, and technology experts. The analysis phase will also consider the various security and privacy implications of the system. This will involve assessing the potential risks and vulnerabilities of the system and developing strategies to mitigate these risks. The analysis will also ensure that the system complies with relevant data protection regulations and standards. In conclusion, the analysis phase will provide a comprehensive understanding of the system's requirements, functionalities, and constraints. This understanding will serve as the foundation for the design, development, and implementation of the fingerprint and iris biometric controlled smart banking machine embedded with GSM technology for OTP.

IVDESIGN OF SYSTEM

The design phase is the stage where the conceptual framework of the system is translated into a practical blueprint, based on the requirements identified during the analysis phase. It outlines how the system will operate, defining its architecture, key components, interactions, and overall structure. For the fingerprint and iris biometric-controlled smart banking machine, this phase includes the design of both hardware and software elements. It involves creating the user interface, establishing the database architecture, and defining communication protocols necessary for secure and efficient system operation.

The design process begins with a high-level architectural overview, identifying the main modules and their roles. This is followed by a more detailed design of individual components, including:

- **Technology Selection**: Choosing appropriate hardware and software platforms.
- **Database Design**: Creating a schema for storing biometric and transaction data securely.
- **User Interface Design**: Developing a simple and intuitive interface for customer interaction.
- **Communication Protocols**: Specifying secure methods for data transmission, especially between the ATM, backend server, and GSM module.

Crucially, the design phase also addresses **security and privacy considerations**, ensuring that the system is resistant to tampering, unauthorized access, and data breaches. The goal is to create a robust, reliable, and user-friendly banking system that provides enhanced protection through biometric authentication.

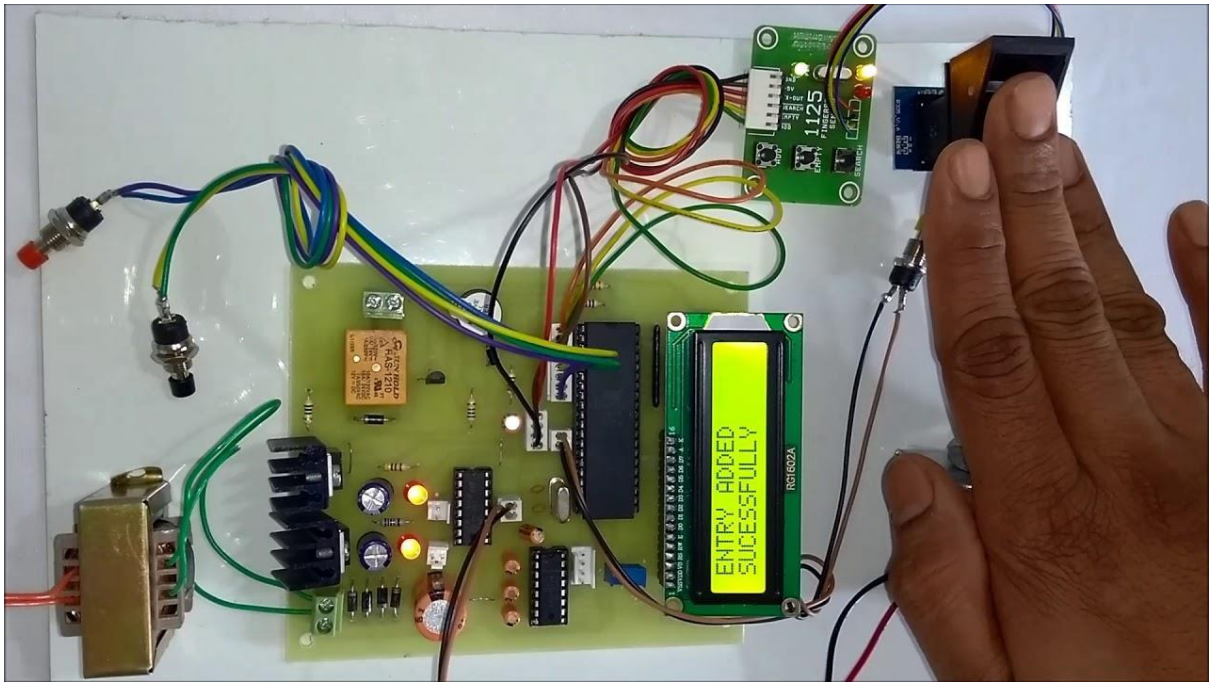

Fig2: Hardware Implementation

V IMPLEMENTATION & RESULTS

The implementation phase involved converting the system design into a fully functional application. This included developing software modules, integrating biometric hardware (fingerprint and iris scanners), connecting a GSM modem for OTP communication, designing a user-friendly interface, and configuring the backend database. Rigorous testing—ranging from unit and integration to system and user acceptance—was conducted to ensure the system performed reliably and securely under various conditions.

Key system functions were implemented with a focus on security and usability. Biometric authentication was achieved using high-resolution sensors and matching algorithms, offering a secure and live-user identification method that replaces traditional PINs. OTP generation and verification were handled through a GSM module, enabling secure, time-sensitive transaction approval. Transaction processing was managed through a secure database and validation logic, ensuring fast and reliable financial operations. The user interface was designed to be intuitive and accessible, featuring visual cues, voice prompts, and tactile feedback to accommodate diverse user needs.

Fig. 13. Transaction Successful

Fig: 3 Resultant image of project

Various forms were developed to facilitate user interaction, including a login form for biometric input, a transaction form to initiate banking actions, and an OTP input form for final authorization. Corresponding output screens provided real-time feedback—such as authentication results, transaction confirmation, and error messages—to guide users throughout their session.

Testing results confirmed high accuracy in biometric matching, rapid OTP delivery and verification, and fast, reliable transaction processing. User feedback was overwhelmingly positive, highlighting the system's ease of use and strong security features. The implementation was carried out using a microcontroller-based platform integrated with biometric sensors, a GSM module, and a secure database, ensuring real-time performance, modularity, and robustness.

VI TESTING & VALIDATION

6.1 Introduction

The testing and validation phase ensured that the system functioned correctly and met user and stakeholder requirements. For the biometric-controlled smart banking machine, testing focused on biometric accuracy, OTP reliability, transaction efficiency, and interface usability. Various scenarios were simulated to assess system robustness, followed by validation through user acceptance testing and stakeholder reviews.

6.2 Design of Test Cases and Scenarios

Test cases were designed to evaluate successful and failed biometric authentication under different conditions, including poor lighting and spoof attempts. OTP testing verified secure and timely delivery, handling both correct and incorrect OTP entries. Transaction processing was tested for accuracy, failures due to invalid inputs or insufficient funds, and concurrent usage. Interface usability was assessed through tests involving users of varied technical backgrounds and accessibility needs. Test scenarios included normal operations, error handling, security breach attempts, and system performance under heavy load.

Fig 4 Testing the devices for biometric identification

6.3 Validation

Validation included User Acceptance Testing (UAT), where real users interacted with the system and provided feedback, confirming its usability and functionality. Stakeholder reviews ensured the system aligned with technical and business requirements, while compliance testing verified adherence to data protection standards. Overall, results confirmed the system was secure, user-friendly, and compliant with relevant regulations, meeting both user expectations and stakeholder goals.

CONCLUSION

The Fingerprint and Iris Biometric Controlled Smart Banking Machine, enhanced with GSM-based OTP generation, offers a secure, user-friendly solution for modern banking. By integrating dual biometric authentication with real-time OTP delivery, the system significantly reduces fraud and unauthorized access. The use of fingerprint and iris recognition ensures accurate, tamper-proof identity verification, while GSM technology adds a dynamic layer of protection. Designed for secure transactions in public spaces like ATMs, this system enhances both security and convenience. Overall, the project demonstrates the powerful potential of combining biometrics with mobile communication to safeguard future banking operations and improve user confidence.

REFERENCES

[1] K. Jain, S. Pankanti, S. Prabhakar, H. Lin, and A. Ross, “Biometrics: a grand challenge”, Proceedings of the 17th International Conference on Pattern Recognition (ICPR), vol. 2, pp. 935-942, 2004.M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[2] P. Corcoran and A. Cucos, “Techniques for securing multimedia content in consumer electronic appliances using biometric signatures,” IEEE Transactions on Consumer Electronics, vol 51, no. 2, pp. 545- 551, May 2005.

[3] P. J. Phillips, A. Martin C. L. Wilson and M. Przybocki, “An Introduction to Evaluating Biometric Systems,” IEEE Computer, Vol.33, No.2, Feb. 2000, pp. 56-63.

[4] S. Pankanti, R. M. Bolle and A. Jain, "Biometrics: The Future of Identification," IEEE Computer, Vol.33, No.2, Feb. 2000, pp. 46-49.

[5] H. Lee, S. Lee, T. Kim, and HyokyungBahn, "Secure user identification for consumer electronics devices," IEEE Transactions on Consumer Electronics, vol.54, no.4, pp.1798- 1802, Nov. 2008.

[6] Wang, J. Li, and G. Memik, "User identification based on finger vein patterns for consumer electronics devices", IEEE Transactions on Consumer Electronics, vol. 56, no. 2, pp. 799- 804, 2010.

[7] Mulyono and S. J. Horng, "A study of finger vein biometric for personal identification", Proceedings of the International Symposium Biometrics and Security Technologies, pp. 134- 141, 2008.

[8] Y. G. Dai and B. N. Huang, "A method for capturing the fingervein image using non uniform intensity infrared light", Image and Signal Processing, vol.4, pp.27-30, 2008.