International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

BIOMETRIC ASSISTED SMART CARD FRAME WORK FOR SECURE CAMPUS ACCESS AND CASHLESS PAYMENTS

Dr.B.Mahesh Babu,K.Purnima,Ch.Sai Prasad, B.Mohan Subhash, K.Bhagath

Department of Electrical & Electronics Engineering

Sheshadri Rao Gudlavalleru Engineering college, Gudlavalleru, Krishna District,

Pin code-521356, AP.

Keywords

Biometric Authentication
Smart Card System
RFID Technology
Fingerprint Recognition
Raspberry Pi
Campus Security
Cashless Transactions
Access Control
NFC Technology
Embedded System
Automation
Secure Identification
Thermal Printing
Library Management System
Canteen Payment System

ABSTRACT

This work presents a prototype of a biometric-assisted smart card system developed to improve security and simplify daily operations within a campus environment. The proposed framework combines fingerprint authentication with contactless card technology to ensure that only authorized users can access services and facilities. A fingerprint sensor is used to verify user identity, while an RFID-based smart card system enables quick and convenient interaction across different campus services.The system is built around a compact processing unit that coordinates all operations and manages data flow between components. It is designed to operate in multiple modes, including classroom access, library management, and canteen payments. Users can switch between these modes using a simple interface, and additional verification methods such as password entry are included where required for enhanced security.For library and canteen applications, RFID cards are used for identification, making transactions faster and reducing manual effort. A thermal printing unit is included to generate instant receipts for transactions, improving transparency and record-keeping. All components are powered through a stable low-voltage supply to ensure reliable operation.

Overall, the system offers a unified and efficient solution for campus management by combining biometric verification with smart card technology. It aims to reduce unauthorized access, minimize manual processes, and provide a seamless experience for users across different campus service

INTRODUCTION

In today's rapidly evolving technological world, educational institutions are increasingly adopting smart solutions to improve both security and operational efficiency within campus environments. With the continuous growth in student population and the expansion of campus facilities, managing access control and handling daily transactions has become more complex. Traditional methods such as physical identity cards, manual attendance systems, and cash-based transactions are still widely used, but they come with several limitations. These systems are often time-consuming, less secure, and prone to misuse. Identity cards can be easily lost, duplicated, or shared among individuals, leading to unauthorized access. Similarly, manual processes increase the chances of human error and make real-time monitoring difficult.

Another major concern with conventional systems is the lack of integration between different campus services. Access control, library management, and canteen transactions are usually handled as separate systems, which results in inefficiency and increased administrative workload. There is no centralized mechanism to track user activities or maintain accurate records in real time. Cash-based transactions further reduce transparency and accountability, making it difficult to manage financial data effectively. These challenges highlight the need for a modern solution that can provide better security, faster processing, and improved system coordination.

To overcome these issues, advanced technologies such as biometric authentication and smart card systems have gained significant attention. Biometric technology uses unique physical characteristics, such as fingerprints, to verify the identity of individuals. Since these features are unique to each person, they offer a much higher level of security compared to traditional identification methods. By integrating biometric authentication into campus systems, it becomes possible to eliminate identity fraud and ensure that only authorized users can access restricted areas. This not only improves safety but also builds a more reliable and trustworthy system.

In addition to biometric security, the use of contactless smart card technology further enhances system functionality. Smart cards, based on RFID or NFC technology, enable quick and efficient data exchange between the user and the system. These cards can be used for multiple purposes, such as accessing facilities, borrowing books, and making cashless payments in canteens. The contactless nature of these cards ensures convenience and reduces transaction time, making the system user-friendly and efficient. Combining smart cards with biometric verification creates a multi-layered security approach, which significantly strengthens the overall system.

The proposed system in this project focuses on developing a biometric-assisted smart card framework that integrates multiple campus services into a single platform. It utilizes a fingerprint sensor for secure user authentication and a smart card reader for contactless identification and transactions. The entire system is controlled by an embedded processing unit, which manages communication between hardware components, processes user data, and ensures smooth operation. Additional features such as keypad-based password input and receipt generation further enhance system security and transparency.

One of the key advantages of this system is its ability to unify different campus operations. Instead of maintaining separate systems for attendance, library management, and

payments, the proposed framework combines all these services into one centralized system. This integration reduces complexity, minimizes manual effort, and allows administrators to monitor activities more effectively. Real-time data processing enables accurate record-keeping and quick decision-making, which improves overall system performance.

Moreover, the system promotes the concept of a cashless campus by replacing traditional payment methods with secure digital transactions. Cashless systems not only reduce the risk of financial mismanagement but also provide better tracking of transactions. This ensures transparency and accountability in all financial activities within the campus. At the same time, automation reduces waiting time and improves the user experience for students and staff.

The scalability of the proposed system makes it suitable for future expansion and integration with emerging technologies. As institutions continue to evolve, this framework can be extended to include additional features such as online monitoring, mobile application integration, and cloud-based data storage. Its flexible design allows it to adapt to changing requirements, making it a long-term solution for smart campus development.

In conclusion, the integration of biometric authentication with smart card technology provides an effective solution to the limitations of traditional campus systems. It enhances security by ensuring accurate user identification, improves efficiency through automation, and simplifies operations by integrating multiple services into a single platform. By adopting such advanced systems, educational institutions can move towards a more secure, transparent, and technologically advanced environment.

2. LITERATURE SURVEY

In recent years, the development of smart campus systems has gained considerable attention due to the increasing need for secure, automated, and efficient management solutions in educational institutions. Researchers have explored various technologies such as biometrics, RFID, smart cards, and IoT-based systems to overcome the limitations of traditional manual methods. These studies mainly focus on improving identity verification, reducing human effort, and enhancing system reliability.

Biometric authentication has emerged as one of the most reliable methods for user identification. Unlike passwords or ID cards, biometric traits such as fingerprints are unique to each individual and cannot be easily shared or duplicated. Several research works highlight that biometric systems significantly improve security by ensuring accurate user verification and preventing unauthorized access. At the same time, researchers emphasize that proper handling and protection of biometric data are essential to avoid privacy risks and misuse.

RFID technology is another widely studied solution for automation in campus environments. It enables quick and contactless identification using radio frequency signals, making it suitable for applications like attendance monitoring, access control, and library management. Studies show that RFID systems reduce time consumption and simplify operations by automatically capturing user data without manual intervention. However, RFID alone has certain limitations, such as the possibility of card loss, duplication, or misuse, which can compromise system security.

To address these limitations, many researchers have proposed combining RFID with biometric authentication to create hybrid systems. These systems use both a physical card and a unique biometric trait for verification, providing a higher level of security compared to single-factor systems. Experimental studies indicate that such integration reduces identity fraud and ensures that only genuine users can access the system. Additionally, hybrid systems improve accuracy and maintain data integrity while keeping the system efficient and user-friendly.

Smart card technology has also been extensively used in secure authentication systems. Smart cards can store user information securely and support encrypted communication, making them suitable for applications like financial transactions and access control. Researchers suggest that when smart cards are combined with biometric verification, the overall system becomes more robust and resistant to security threats. This combination forms the basis of multi-factor authentication systems, which are now widely considered as a standard approach for high-security applications.

Recent studies have further explored multi-factor authentication frameworks that integrate biometrics, smart cards, and passwords. These systems provide multiple layers of verification, making them more secure against unauthorized access and cyber threats. Modern research also highlights the role of advanced algorithms and intelligent systems in improving the accuracy and speed of biometric recognition, thereby enhancing overall system performance.

In addition, IoT-based and automated campus systems have been studied for their ability to provide real-time monitoring and centralized data management. These systems reduce manual workload, improve transparency, and ensure accurate record-keeping. Research findings indicate that automation not only increases efficiency but also helps institutions manage large-scale operations more effectively. However, challenges such as system cost, data security, and scalability still need to be addressed for wider implementation.

Overall, the existing literature clearly shows that while individual technologies like RFID, biometrics, and smart cards offer specific advantages, their integration provides a more effective and reliable solution. Hybrid systems combining these technologies achieve better security, improved efficiency, and enhanced user convenience. Based on these insights, the proposed biometric-assisted smart card framework aims to utilize the strengths of these technologies to develop a secure, integrated, and scalable system for modern campus environments.

3.1 PROBLEM IDENTIFICATION

The rapid growth of educational institutions has increased the complexity of managing campus operations effectively. However, many campuses still rely on outdated methods for access control and transaction handling, which creates several operational and security-related challenges. These conventional approaches are no longer capable of meeting the demands of a modern, technology-driven environment.

A primary concern lies in the weakness of existing identification systems. The use of physical ID cards as the main authentication method does not provide sufficient security, as these cards can be easily misplaced, duplicated, or misused by others. This limitation makes it difficult to ensure that access to restricted areas is granted only to authorized individuals, thereby increasing the risk of unauthorized entry.

Another critical issue is the fragmented nature of campus services. Functions such as classroom access, library operations, and canteen payments are typically handled through separate systems that do not communicate with each other. This lack of integration leads to inefficiencies, as data must be managed independently for each service. As a result, administrators face difficulties in maintaining consistency, monitoring activities, and generating accurate reports.

The dependency on manual processes further adds to the problem. Tasks such as attendance marking, transaction recording, and resource management are often performed manually, which not only consumes time but also increases the likelihood of human errors. These inefficiencies can lead to delays, inaccurate data, and reduced productivity across the campus.

In addition, cash-based transactions continue to be widely used, especially in campus canteens and small-scale services. This approach introduces challenges such as slow processing, lack of proper transaction tracking, and the possibility of financial discrepancies. Without a digital system, ensuring transparency and accountability becomes difficult.

Security is also limited due to the absence of multi-level authentication mechanisms. Most existing systems rely on a single form of verification, which is not sufficient to prevent identity misuse or fraud. The lack of advanced authentication methods reduces the overall reliability of the system and makes it vulnerable to unauthorized access.

Data management is another area of concern. Information is often stored in isolated systems without real-time updates, making it hard to retrieve accurate and up-to-date records. This not only affects operational efficiency but also limits the ability of administrators to make informed decisions.

Considering these challenges, it is evident that the current systems are inadequate in providing a secure, efficient, and integrated solution for campus management. There is a clear need for a system that combines advanced authentication, automation, and centralized control to improve overall performance and ensure a safer campus environment.

3.2 SCOPE OF THE PROJECT

The scope of this project is to develop a secure and efficient campus management system using biometric authentication and smart card technology. It focuses on providing controlled access to campus facilities through fingerprint verification, ensuring that only authorized users are allowed entry.

The system also enables cashless transactions using RFID/NFC-based smart cards, which improves speed, accuracy, and transparency in payments. In addition, it supports basic library operations by allowing quick identification of users and resources.

The project integrates multiple campus services into a single platform, reducing manual work and improving overall efficiency. It is designed as a scalable prototype that can be expanded in the future with advanced features and wider implementation.

4. METHODOLOGY & MODELLING

The proposed system is designed to provide a secure and integrated solution for campus access and cashless transactions by combining biometric authentication with smart card technology. The methodology follows a structured approach that includes system design, hardware integration, software development, and real-time operation.The overall system is divided into two main sections: the **user authentication unit** and the **processing and control unit**. The user authentication unit is responsible for verifying the identity of users through multiple inputs, while the processing unit manages decision-making and system coordination.

The process begins with **user identification**. When a user interacts with the system, the fingerprint sensor captures the biometric data and compares it with the stored database. If the fingerprint matches, the user is considered valid. In addition to biometric verification, a smart card is used for identification through an RFID/NFC reader. This ensures that both the user and the card are authenticated, providing an extra layer of security.Once the user is authenticated, the system allows access to different operational modes such as classroom entry, library services, or canteen transactions. A push button is used to select the required mode, and a keypad is provided for entering passwords when additional security is needed. This creates a **multi-factor authentication mechanism**, which enhances system reliability and prevents unauthorized usage.

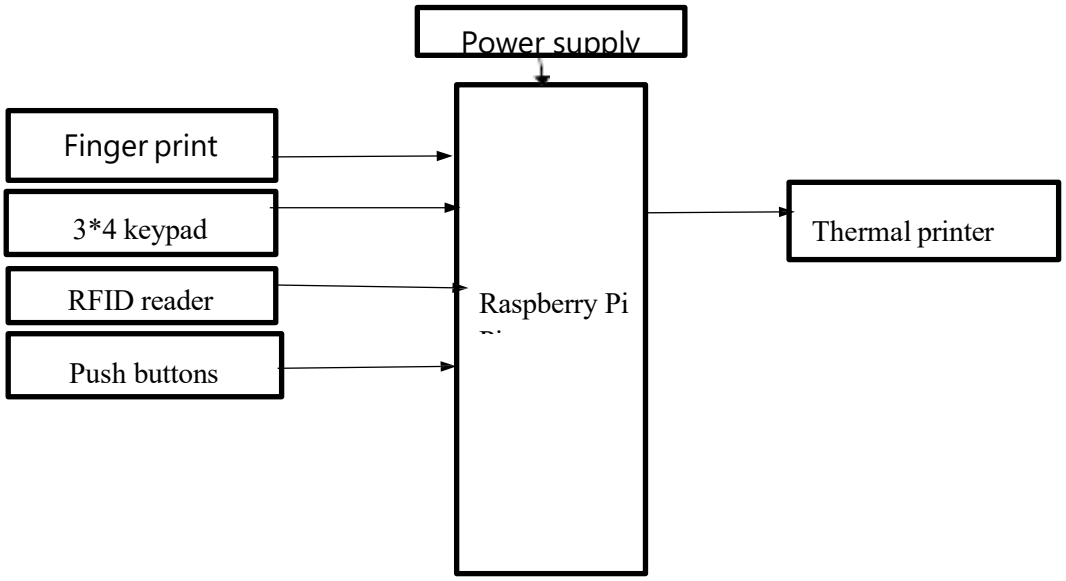
The **central processing unit**, built around an embedded controller, receives input data from all connected devices and processes it based on predefined logic. It controls access decisions, manages transaction records, and coordinates communication between components. The system software is developed to handle tasks such as fingerprint matching, card detection, data validation, and output generation.For **cashless transactions**, the smart card stores user-related information and balance details. When a transaction is performed, the system verifies the card, processes the payment, and updates the records accordingly. A thermal printer is used to generate receipts, ensuring transparency and proper documentation of transactions.

From a modelling perspective, the system can be represented as a sequence of interconnected modules. The input layer includes the fingerprint sensor, RFID reader, keypad, and mode selector. These inputs are processed by the central controller, which acts as the decision-making unit. The output layer includes access control signals and transaction outputs such as printed receipts or display messages.

The system operates in a **real-time environment**, where inputs are continuously monitored, and responses are generated instantly. Proper synchronization between hardware and software ensures smooth functioning. The design is modular, allowing easy modification or expansion of system components in the future.

Overall, the methodology emphasizes secure authentication, efficient data processing, and seamless integration of multiple campus services. The modelling approach ensures clarity in system design and supports reliable implementation of the proposed framework.

Fig 1. Block Diagram



Additionally, the design follows a **modular approach**, where each component functions independently but is connected through a central system. This makes it easier to upgrade or modify individual modules without affecting the overall system performance. The modular structure also supports scalability, allowing the system to be expanded with new features such as online monitoring or mobile integration in the future.

Error handling and data validation are also important parts of the methodology. The system is programmed to detect invalid inputs, authentication failures, and communication errors. Appropriate responses are generated to ensure system reliability and user awareness. This improves overall system robustness and reduces the chances of malfunction.

In summary, the methodology focuses on integrating biometric authentication, smart card technology, and embedded system control into a unified framework. The modelling approach clearly defines the interaction between different components and ensures smooth system operation. This structured design not only enhances security and efficiency but also provides a flexible foundation for future improvements and large-scale implementation.

Fig 2.

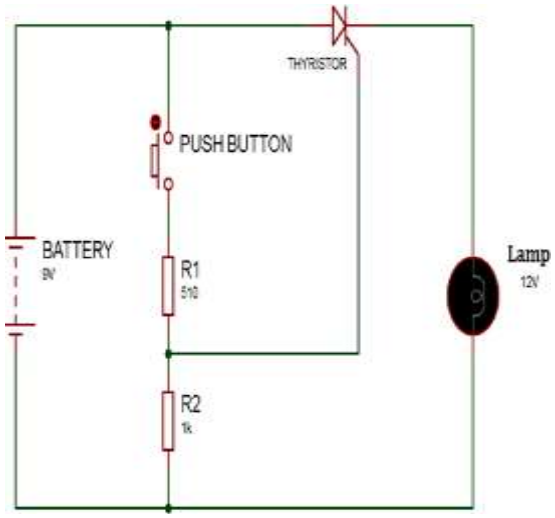


Fig 3.

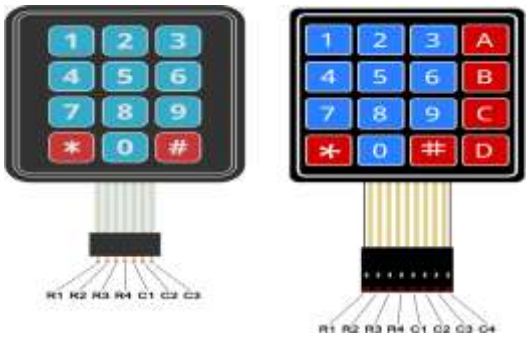


Fig 4

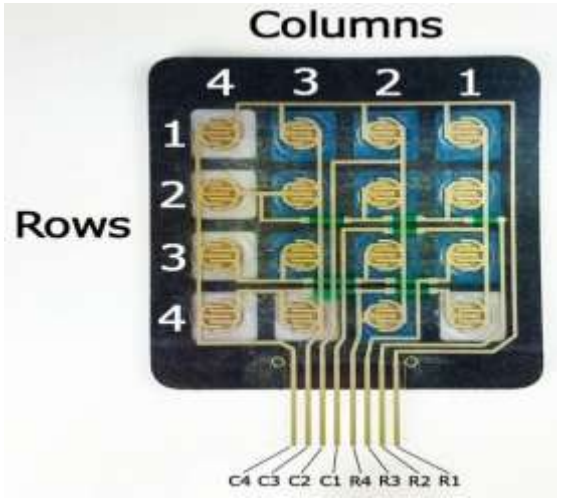
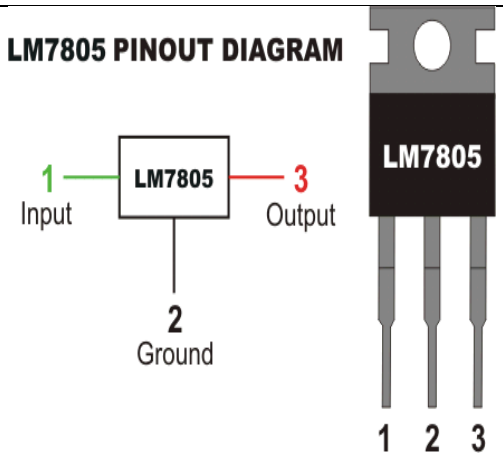


Fig 5

Fig 6	Fig 7
	
Fig 8	Fig 9
	
Fig 10	Fig 11

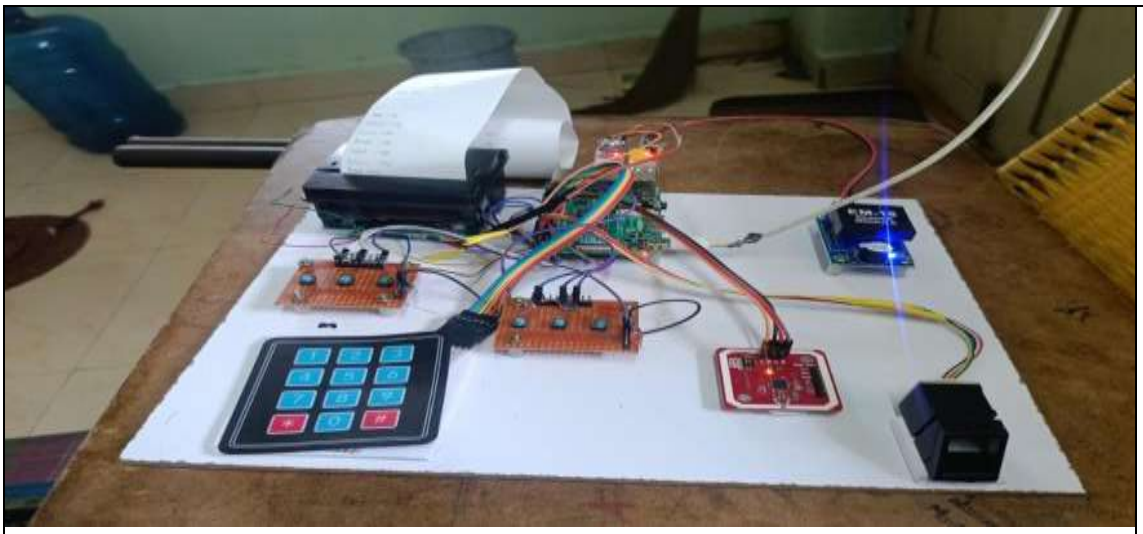


fig 12

5. CONCLUSION

The proposed biometric-assisted smart card framework provides an effective solution to the limitations of traditional campus management systems. By combining fingerprint-based authentication with smart card technology, the system ensures a higher level of security and prevents unauthorized access. The use of multi-factor authentication further strengthens reliability by verifying both the user identity and the associated card information.

The integration of multiple services such as classroom access, library management, and canteen transactions into a single platform improves overall efficiency and reduces manual effort. The implementation of cashless transactions enhances transparency, minimizes errors, and simplifies financial handling within the campus. Real-time processing and automated record management contribute to better monitoring and control of daily activities.

The system is designed with a modular and scalable approach, allowing future enhancements and easy adaptation to evolving requirements. It demonstrates how embedded systems and modern authentication technologies can be effectively used to create a smart and secure campus environment.

Overall, the project successfully achieves its objective of developing a reliable, efficient, and user-friendly system that enhances security, streamlines operations, and supports the transition towards a fully automated and cashless campus.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, “An Introduction to Biometric Recognition,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, Jan. 2004.

[2] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 3rd ed., Wiley, 2010.

[3] S. Garfinkel and B. Rosenberg, *RFID: Applications, Security, and Privacy*, Addison-Wesley, 2005.

[4] NXP Semiconductors, “PN532 NFC Controller Datasheet,” 2019.

[5] Raspberry Pi Foundation, “Raspberry Pi 4 Model B Datasheet,” 2020.

[6] A. Juels, “RFID Security and Privacy: A Research Survey,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381–394, Feb. 2006.

[7] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, 2nd ed., Springer, 2009.

[8] S. Kumar and D. Zhang, "Personal Recognition Using Hand Shape and Texture," *IEEE Transactions on Image Processing*, vol. 15, no. 8, pp. 2454–2461, Aug. 2006.

[9] M. A. Ferrag, L. Maglaras, H. Janicke, and J. Jiang, "Authentication Protocols for Smart Cards: A Review," *IEEE Access*, vol. 6, pp. 10927–10944, 2018.

[10] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classifying RFID Attacks and Defenses," *Information Systems Frontiers*, vol. 12, no. 5, pp. 491–505, 2010.

AUTHOR DETAILS:

AUTHOR-1	**NAME**:Dr.B.Mahesh Babu Associate Professor **E.mail:**bannu219@gmail.com
AUTHOR-2	**Name:**K.Purnima **ROLL NO:** 22481A0238 **E-Mail:**konathampurnima@gmail.com
AUTHOR-3	**Name:**CH.Sai Prasad **ROLL NO:** 22481A0208 **E-Mail**: saichilukoti7777@gmail.com

AUTHOR-4	**Name:** B.M.Subhash **ROLL NO:** 22481A0207 **E-Mail:**bommasanimohansubhash@gmail.com
AUTHOR-5	**Name:**B.Bhagath **ROLL NO:** 22481A0236 **E-Mail:**bhagathk7702@gmail.com