



Smart ID Card with Location Based Access Control System

Dudekula Hajurun, Kadavakallu Bhanu Prakash Reddy, Guntipalli.Bharath, Gondi Latha, Devarakonda Bhaswanth

Department of Computer Science and Engineering, Gates Institute of Technology, Andhra Pradesh, India.

Correspondence

Dudekula Hajurun

Department of Computer Science and Engineering, Gates Institute of Technology, Andhra Pradesh, India.

Abstract

The Smart ID Card with Location-Based Access Control system is an advanced security solution designed to enhance traditional access control mechanisms by integrating real-time location verification. Unlike conventional systems that rely solely on identity validation, this system incorporates GPS-based authentication to ensure that users are physically present within authorized zones before granting access. The system compares real-time latitude and longitude data with predefined locations stored in a database, thereby preventing misuse of lost or stolen ID cards. The architecture includes a web-based frontend developed using HTML, CSS, and JavaScript, a backend implemented using Spring Boot, and a MySQL database for storing user information and access logs. This approach improves security, accountability, and operational efficiency while supporting scalability for future enhancements.

- Received Date: 11 Feb 2026
- Accepted Date: 02 Apr 2026
- Publication Date: 25 Apr 2026

Keywords

Smart ID Card, Location-Based Access Control, GPS, Authentication, Security

Introduction

Access control systems are a fundamental component of organizational security, ensuring that only authorized individuals can access restricted resources, locations, or information. Traditional access control mechanisms rely heavily on physical ID cards, RFID systems, or biometric verification. While these methods provide a basic level of security, they are vulnerable to several limitations such as card theft, duplication, and unauthorized sharing. With the increasing need for secure and intelligent systems, there is a growing demand for access control mechanisms that go beyond simple identity verification. One of the major limitations of existing systems is the inability to verify the real-time physical presence of the user. This gap can lead to serious security breaches, especially in organizations with distributed locations or sensitive environments.

The proposed Smart ID Card with Location-Based Access Control system addresses these challenges by integrating Global Positioning System (GPS) technology into the authentication process. This system ensures that access is granted only when the user is physically present within a predefined geographical boundary. By combining identity verification with location validation, the system enhances overall security and minimizes the risk of unauthorized access. Furthermore, the system leverages modern web technologies and backend frameworks to provide a scalable and efficient solution. It also maintains detailed logs for monitoring

and auditing purposes, making it suitable for enterprise-level deployment.

In today's digital world, security has become one of the most important concerns for organizations. With the increasing number of cyber threats and physical security breaches, it is necessary to develop systems that provide both accuracy and reliability. Traditional access control systems mainly focus on verifying "who the user is," but they fail to verify "where the user is." This limitation can lead to serious misuse of access privileges.

Related Work

Several research studies and existing systems have attempted to improve access control mechanisms using technologies such as RFID, biometric authentication, and QR code-based systems. RFID-based systems are widely used due to their ease of implementation and cost-effectiveness. However, they are prone to cloning and unauthorized usage. Biometric systems, including fingerprint and facial recognition, offer improved security but come with challenges such as high implementation cost, privacy concerns, and dependency on hardware reliability. Additionally, these systems still lack location awareness, which is critical in certain applications. Recent advancements have explored the use of mobile-based authentication and geofencing techniques. Geofencing allows systems to define virtual boundaries and trigger actions when a user enters or exits a specific area. However, many existing implementations are limited in scalability and lack integration with centralized access control systems.

Copyright

© 2026 Authors. This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International license.

Citation: Dudekula H, Kadavakallu BPR, Guntipalli B, Gondi L, Devarakonda B. Smart id Card with Location Based Access Control System . GJEIIR. 2026;6(4):228.

Proposed System

The proposed system is designed as a multi-layered architecture that integrates frontend interfaces, backend processing, and database management with real-time location tracking.

The proposed system is designed to provide a secure and efficient access control mechanism by combining multiple technologies. It uses GPS-based location tracking along with traditional authentication methods to ensure accurate verification.

The system uses REST APIs for communication between frontend and backend. Data is transmitted securely using encryption techniques to prevent unauthorized access or data tampering.

The backend system processes requests in real time and ensures minimal delay in granting or denying access. The use of scalable frameworks like Spring Boot allows the system to handle multiple users simultaneously without performance issues.

Additionally, the system supports dynamic configuration of authorized locations. Administrators can easily update or modify access zones based on requirements. This flexibility makes the system adaptable to different environments.

Error handling and validation mechanisms are also implemented to ensure smooth system operation even in unexpected situations such as GPS failure or network issues.

System Workflow

The process begins when a user attempts to access a secured system or location. The user provides their ID credentials through a web or mobile interface. Simultaneously, the system captures the user's real-time geographical coordinates using GPS technology. These coordinates, along with the user ID, are sent to the backend server via secure API communication. The backend system processes this information by first verifying the user's identity against the database. Once authenticated, the system compares the user's current location with predefined authorized zones stored in the database. If the user's location falls within the permitted range, access is granted. Otherwise, the system denies access and logs the attempt for further analysis.

System Architecture

The system architecture consists of three primary layers:

Frontend Layer: Developed using HTML, CSS, and JavaScript, this layer provides an interactive interface for users to input credentials and initiate access requests.
Backend Layer: Implemented using Spring Boot, this layer handles business logic, authentication, and communication with the database.
Database Layer: MySQL is used to store user data, authorized locations, and access logs.

Modules Description

Employee Management Module manages user details such as ID, name, and assigned access levels. **Location Management Module** stores and updates authorized geographical zones using latitude and longitude values. **Access Control Module** performs real-time verification of user identity and location. **Logging Module** records all access attempts, including successful and failed entries, along with timestamps and location data.

Advantages of Proposed System

The integration of GPS technology ensures that access control is not only identity-based but also context-aware. This

significantly reduces the chances of unauthorized access and enhances system reliability. management, location management, access verification, and access logging. The architecture includes a frontend interface developed using web technologies, a backend server using Spring Boot, and a MySQL database for storing user data, location information, and access logs.

Results And Discussion

The performance of the system was evaluated under different conditions to ensure reliability and accuracy. The system showed consistent results in detecting user location and validating access requests.

During testing, the GPS module provided accurate location data within an acceptable margin of error. The backend system efficiently processed requests and responded within a short time, ensuring a smooth user experience.

The system also demonstrated the ability to handle multiple requests simultaneously without performance degradation. Logging features provided detailed insights into system activity, which is useful for analysis and monitoring.

Compared to traditional systems, the proposed system significantly reduces the chances of unauthorized access. It also improves transparency by maintaining detailed records of all access attempts.

Future Work

The system can be further enhanced by introducing additional features and technologies. One major improvement is the development of a mobile application, which will make the system more accessible and user-friendly.

Integration with Internet of Things (IoT) devices such as smart locks and sensors can automate access control processes. Artificial Intelligence (AI) can be used to analyze user behaviour and detect unusual activities.

The system can also be expanded to support multiple locations and dynamic access policies based on time, role, or activity. Cloud integration can improve scalability and allow remote monitoring.

Another enhancement is the use of advanced location technologies such as Wi-Fi positioning and Bluetooth beacons for improved accuracy in indoor environments.

System design

The system design follows a modular and layered approach, which improves maintainability and scalability. Each component of the system performs a specific function and communicates with other components through well-defined interfaces.

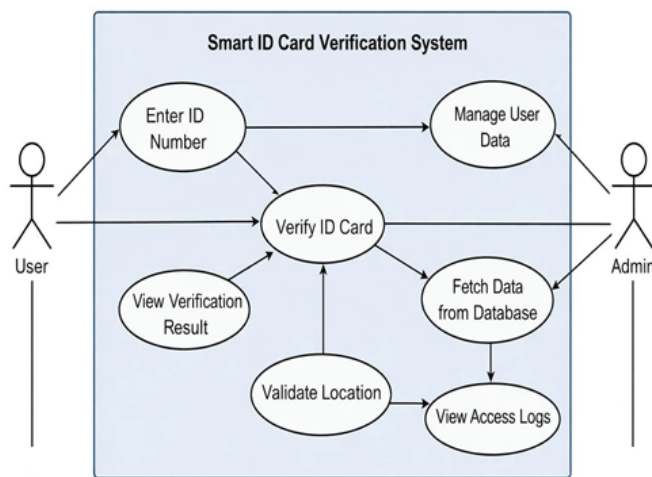
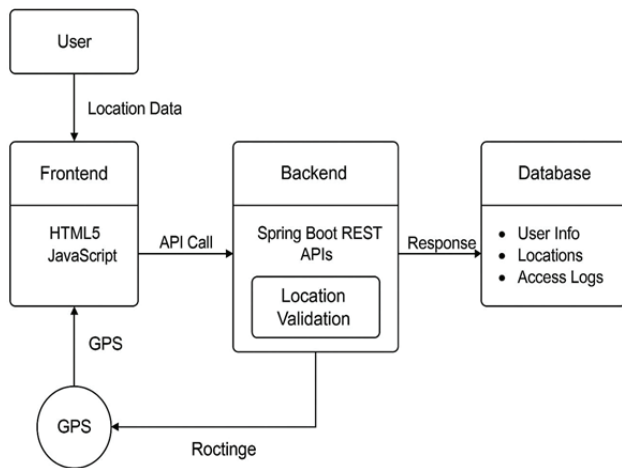
The frontend is designed to be simple and user-friendly, allowing users to easily enter credentials and request access. It also uses browser-based geolocation services to capture real-time location data.

The backend acts as the core of the system, where all processing takes place. It validates user credentials, processes location data, and makes access decisions based on predefined rules.

The database is structured to store user details, location coordinates, and access logs efficiently. Index techniques are used to improve query performance. Security measures such as data encryption, secure APIs, and authentication tokens are implemented to protect sensitive information.

Security

- Security is a critical aspect of the proposed system. Multiple layers of security are implemented to ensure



maximum protection against unauthorized access.

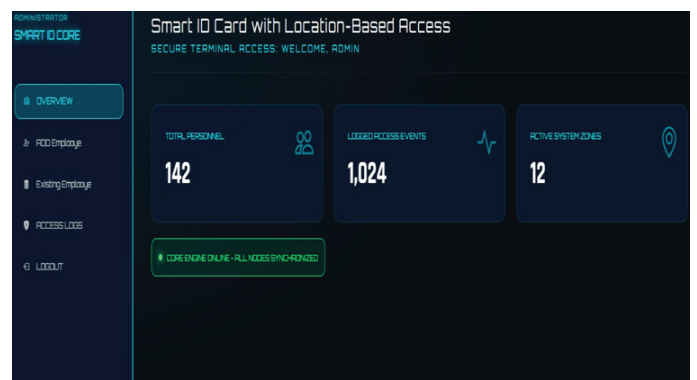
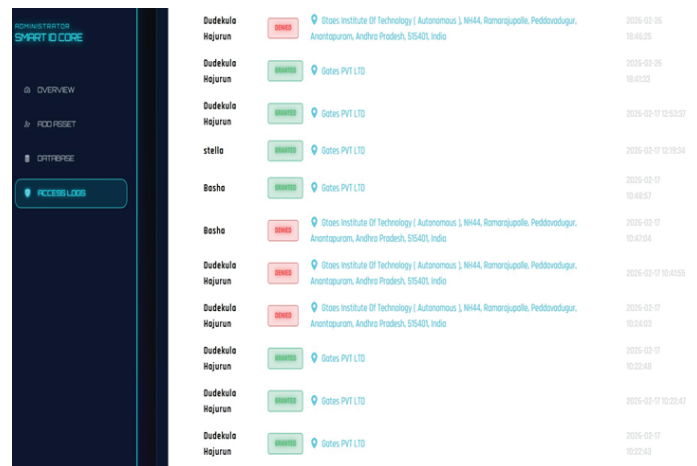
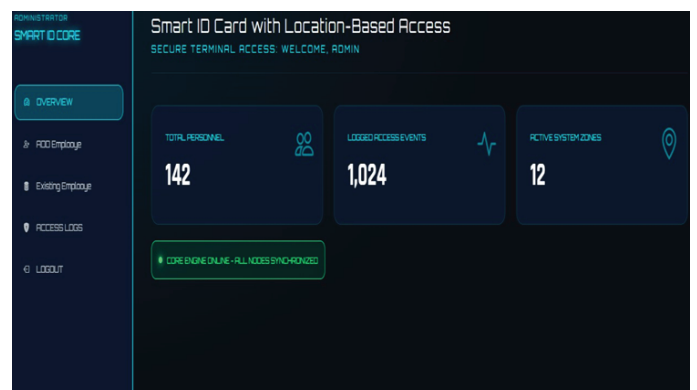
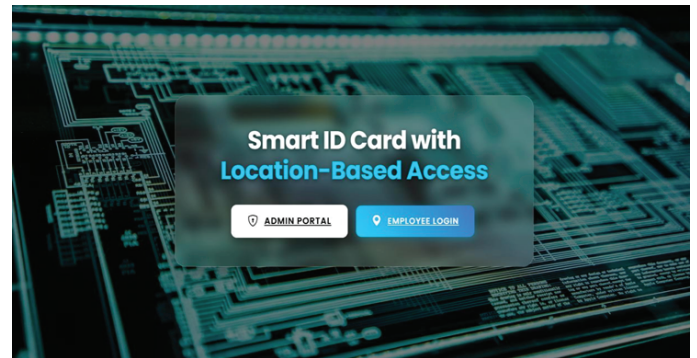
- The first layer involves user authentication, where credentials are verified against the database. The second layer involves location verification, ensuring the user is physically present in the authorized area.
- The system also includes secure communication protocols to protect data during transmission. Encryption techniques are used to prevent data interception and misuse.
- Logging mechanisms track all activities, allowing administrators to monitor system usage and detect suspicious behavior. Alerts can also be generated for repeated unauthorized access attempts.
- These security measures make the system highly reliable and suitable for sensitive environments.

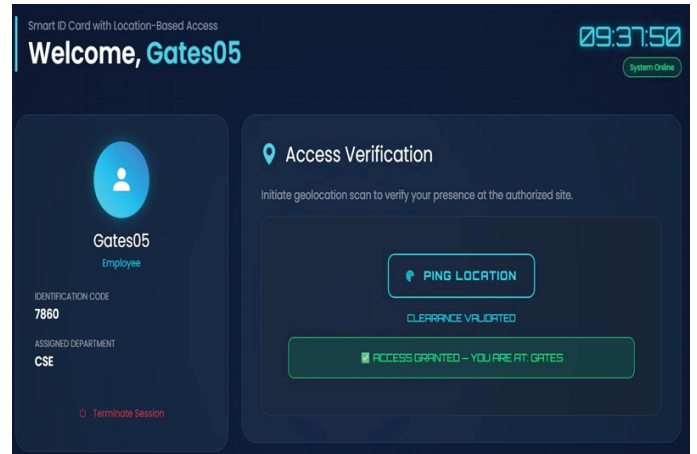
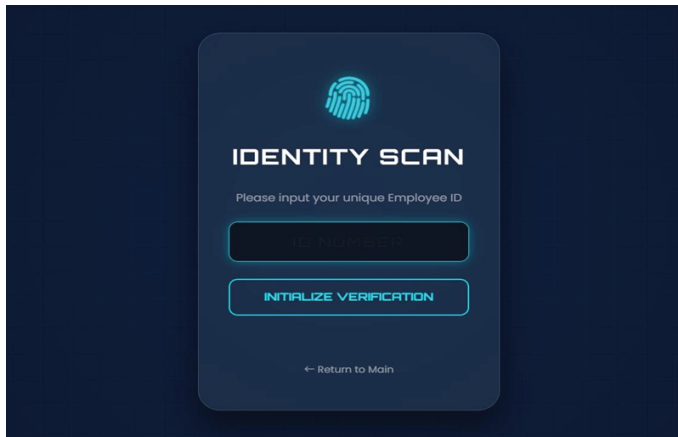
Conclusion

The Smart ID Card with Location-Based Access Control system represents a significant advancement in access management solutions. By integrating GPS-based location verification with traditional identity authentication, the system ensures a higher level of security and reliability. The system effectively addresses the limitations of existing access control mechanisms by preventing unauthorized access through stolen or misused ID cards. It also enhances operational efficiency by automating the verification process and maintaining comprehensive access logs.

Overall, the proposed system provides a scalable, secure,

and intelligent solution suitable for modern organizations. Its adaptability and potential for future enhancements make it a valuable contribution to the field of access control systems.





References

1. Smart ID Card with Location Based Access Control Project Report
2. Spring Boot Documentation
3. MySQL Documentation
4. HTML, CSS, and JavaScript Documentation