



# CAMPUS CONNECT

**Mr. Pratharv Surve, Mr. Shoaib Sarkare, Mr. Parth Kadam**  
Assistant Professor, Undergraduate Student, Undergraduate Student  
Department of Information Technology  
University of Mumbai, Mumbai, India

**Abstract:** One active challenge in educational institutions as of operation manuals relates to the manual processing of student identification verification. When students lack their physical identification cards, they are forced to go through time-consuming processes, such as writing formal applications, administrative approvals or facing temporal entry restrictions. This predicament engenders that piece of administrative inefficiencies, precipitates delays at campus entry points, and imposes upon students and faculty unnecessary inconvenience.

To address these problems, the present project is aimed at introducing Campus Connect, a web-based digital platform designed to simplify campus access management. The system empowers students who have misplaced their ID cards to generate a secure, temporary one day electronic ID using facial verification and minimal payment of a nominal fine process. By providing a central point of API connecting pupils to administrators, the platform ensures real-time validation and controlled access to facilities on campus.

Students are allowed to authenticate their own identity, make the necessary payment and then a digital electronic identification card containing their name, roll number, course, year, their photograph, and date of validity can be created and provided to them.

The administrative panel is used to efficiently register students, upload data in bulk using CSV and monitor issued temporary IDs.

By automating the verification and approval process, Campus Connect removes manual paperwork, alleviates entry point congestion, increases security, and increases overall campus operational efficiency. The system enables the promotion of digital transformation within the educational institutions and supports a structured transparent and technology-driven campus environment.

**Index Terms:** *Campus connectivity, Digital identity management, temporary electronic identification, facial authentication, Campus access control, Web application, administration automation, Student information system, Digital campus transformation.*

## I. INTRODUCTION

### A. Background

Educational institutions often face operational inefficiencies that are caused by manual identity verification procedures. When students fail to bring possession of their physical identification cards, the institution imposes onerous processes (including the submission of written applications and the solicitation of approvals) that result in delays and increased administrative workloads. This situation makes the need for a technologically sophisticated intelligent solution for campus access management imperative.

In many Indian colleges, a lack of digital verification mechanism creates wastage of inconvenience for all concerned and also brings potential security risks to the colleges. A smooth digital platform can eliminate the administrative paperwork and synchronous authentication can be achieved.

Campus Connect represents a web-based system designed to simplify the entry management for campuses. The platform allows students to validate who they are - via facial recognition - send a nominal fine, and immediately generate a secure, one day valid electronic ID card. Administrators can control datasets of students, enrol new students and track temporary ID issuance via a centralized dashboard.

Digitization of this process in the form of Campus Connect contributes to the overall strengthening of security on campus, reduce the administrative workload and create a well-structured, efficient and modern campus environment.

**B. Problem Statement**

Many institutions of learning are still using manual and paper-based processes for stakeholder identity verification in cases where there are misplaced identification cards. These traditional methods are inefficient, time-consuming and conspicuously lack systematic tracking mechanisms. The deficiencies inherent in the present system can be drawn as follows:

- Firstly, there is lack of a centralized digital platform for issuing temporary identification credentials.
- Secondly, the procedure requires manual approvals, thus causing delays in the access points at the campus.
- Thirdly, there is no real-time monitoring or tracking of students entering premises without having proper identification.
- Fourthly, the system lacks the essential transparency in transparency and the structured record maintenance.
- Finally, predominant procedures are inconvenient and increase administrative burdens.

To accomplish an efficient, secure and transparent management of access to the campus, it is imperative to have a centralized, automated and web-enable infrastructure that verbalizes the identity and the generation of a temporary identification token.

**C. Objectives**

The following objectives have been delineated for the project being proposed:

- To implement a Web-based, automated system for campus access management.
- To create the centralized tool to allow student and administrators to control the issuance of temporary identification.
- To design an automated process for verification of identity and generation of temporary electronic identification.
- To design a safe, trustworthy and easy to use authentication system, including facial verification and payment system.
- To improve the process of real-time monitoring and streamline the campus entrance process for better operational efficiency and security.

**II. PURPOSE AND PROBLEM DEFINITION****A. Purpose of the System**

The main goal of this system is to provide a set organized digital framework that allows for efficient management of access to campus.

The system aims to:

- Streamline the temporary ID issuing by automating work flows.
- Boost campus security through authenticated digital digital authentication
- Decrease the workload of administrative tasks and avoid paper-based operations.
- Increase coordination between students and administration.
- Promote digital transformation in the educational institutions

**B. Operational Challenges**

The system solves some of the operational issues, including:

- Managing simultaneous requests for temporary identification during a period of maximum ingress; and
- Making sure to use real-time authentication and communication between students and administrative personnel is crucial.
- Providing secure authentication based on facial recognition technology in combination with controlled authorization protocols
- Maintaining exact and central records of student data.
- Monitoring and tracking the distribution of temporary electronic ID cards in an efficient manner.

**III. SCOPE****A. Functional Scope**

The system outlines the following modules::

- Student Registration and Logging in Module
- Facial Verification and Facial Authentication Module
- Generating and Validating e-IDs for a limited time.
- Fine Payment and Transaction Management Module
- Admin Panel to Manage and Monitor Students

## B. Technical Scope

- **Frontend:** React.js
- **Backend:** Node.js, Python, OpenCV
- **Database:** MongoDB Atlas
- **Platform:** Web-based Application

## C. Limitations

- Requirement: The internet connectivity must be constant and will be required by real time authentication and e-ID creation.
- Depends on the quality and honesty of the student data prior to registration.
- The accuracy of facial authentication can also be influenced because of lighting and quality of the camera.
- Limited offline features in case of unavailability of the server or network.

## IV. EXISTING SYSTEM / LITERATURE REVIEW

### A. Traditional System for Entry to the Campus

In many educational institutes, student identity verification is taken care of by manual processes. When students forget their ID cards, they have to write applications and seek permissions or go for temporary manual verification at security check post. These methods have lacking structured documentation, centralized tracking and automation leading to delays, administrative burden and inefficiency.

### B. Types of Digital Access Systems that are Existing

Some of the institutions have been implementing basic digital attendance systems or entry mechanisms through an authentication service using radio frequency identification (RFid). However, these systems usually focus on regular ID-based access and do not address the situation when students forget their ID cards. Many lack features of temporary digital ID generation, real-time monitoring, structured database management and integrated administrative control panels.

### C. Research Gap

Existing systems generally:

- Do not offer automated temporary e-ID-generation.
- Do not have a centralized process for monitoring students entering without physical ID cards.
- Have few mechanisms for authentication in real time.
- Provide minimal administrative tracking / reporting capabilities.

The proposed system, Campus Connect, is aimed at filling this gap and establishing a centralized, automated and transparent digital solution for temporary campus access management.

## V. SYSTEM DESIGN AND ARCHITECTURE

### A. Architecture Overview

The system follows a three-layer architecture:

- Presentation Layer: User interface serving students and administrators login and verification & temporary e-ID generation
- Application Layer - Business logic, which includes authentication, handling requests, issuing temporary ID and validating system
- Database Layer: Safe storing & accessing of student data, authentication data & transaction details

### B. Key Modules

- User Authentication Module
- Student registration and profile management Module
- Temporary e-ID generation Module
- Fine Payment and transaction module

- Monitoring and Control Module of Administration

## VI. METHODOLOGY AND ALGORITHMS

### A. Needs Analysis:

Operational difficulties faced by institutions of learning were studied to understand the inefficiencies associated with the manual campus entry system. The needs were analysed by assessing the requirements of the students, security personnel, and administrators to develop a systematic and technology-based access management system.

### B. System Design:

The system design was developed using workflow diagrams, ER diagrams, and database schema designs to develop an efficient data structuring system. The system design is based on secure authentication, temporary e-ID creation, and administrative control.

### C. System Implementation:

The system modules, comprising the frontend and backend systems, were implemented and integrated with the MongoDB database to enable efficient data exchange and secure management of student data and transaction information.

### D. System Test:

The system was tested in the following ways:

- Unit Testing: The module tests were conducted individually, i.e. authentication, temporary e-ID generation, payment processing, and administration modules were individually tested.
- Integration Testing: A combination of all the modules was done and tested as a whole to ensure all modules communicated well in the frontend, backend, and database.
- User Acceptance Testing (UAT): The product was tested by the targeted users so that they could make sure that the system fulfils their functional and usability criteria in addition to living up to the operational expectations in a campus setup.

The testing showed that the system can be relied upon in terms of its operation and consistently keep data on track and also to have all modules interact with each other well.

## VII. IMPLEMENTATION DETAILS

### A. Tech Stack

- Frontend: React.js
- Backend: Node.js , Python
- Database: MongoDB Atlas
- Hosting: Localhost

### B. Security Considerations

- Secure login authentication
- Input validation
- Database protection mechanism
- Role-based access control

## VIII. RESULTS AND DISCUSSION

The system offers an effective resolution to the following:

- Student Registration and Authentication: It is possible to log in and authenticate the students through the system.
- Introduction of temporization of the e-ID: For those students who have lost their physical ID cards, an automated generated temporary e-ID can be created that is one-day valid and a secure way of identification.
- Fine Processing Fine Fine: This platform allows giving the nominal fine online through easy online payment and providing the temporary e-ID.
- Administrative Monitoring: Administrators are able to access student records, add new students and track whenever temporary IDs have been issued to students/students in general with a centralized dashboard.
- Live Tracking and Authentication: The system enables live authentication to be done on issued e-ID cards to curb entry into the campuses.

The application of the above processes has led to a great deal of paper work being eliminated, delays at entry points being minimized, the work between students and administration became a lot more coherent and security and operational effectiveness in the entire campus became enhanced

## B. Result

### Generating E-id Card



Fig 8.1

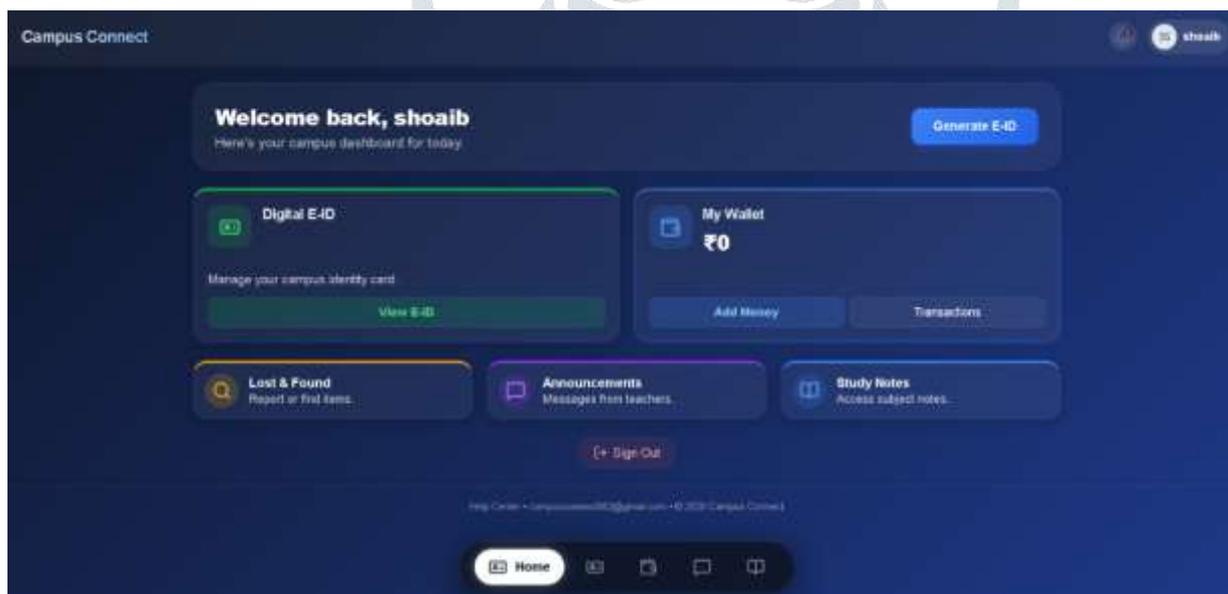


Fig 8.2

## IX. CHALLENGES AND SOLUTIONS

### 1. Reliance on Steady Internet Exploration.

The system needs to have a quick internet connection, to support the process of authentication, real-time e-ID creation, payment, and synchronisation of the database. There can be a transient impact on the system responsiveness and access validation because of network instability.

### 2. Administration Breakdowns in Communication with the students.

Manual systems in place usually result in miscommunication and delays during approval in case students leave their ID cards at home. Campus Connect overcomes this by offering real time status updates and automatic workflow, which enhances coordination and decreases delays at the entry point.

### 3. Student Records Manually Managed.

When working with the data of students manually, it is more probable that the data is subjected to mistakes, repetitions, and poor maintenance of records. The system also uses a properly structured database system to provide proper storage, retrieval, and maintenance of student information.

### 4. Absence of Monitoring and Tracking of Entry.

In the current system, it is not very visible when students get access to campus in the absence of physical id cards. Campus Connect will offer the advantages of centralized surveillance and tracking on issued temporary e-ID cards as a way of increasing transparency and security control.

## IX. CONCLUSION AND FUTURE WORK

Learning institutions need to use efficient, secure, and technology-oriented systems in running their operations. Paper-based identity validation procedures cause delays, more administrative workload and the overall inefficiency of the campus. Campus Connect strives to overcome these issues by providing a structured web-based campus access control service on a temporary basis. The system computerizes identity verification, generates temporary e-ID automatically, provides secure payment processing, and allows administration to control everything within a centralized environment. Campus Connect will tighten the security of campus by helping reduce paperwork, cut paper entry delays and boost real time tracking which would increase efficiency in its operations. The solution evangelizes the phenomenon of digital transformation in educational institutions and creates a scalable system of management in smart campuses.

### *Future Developments*

- Creation of a specific mobile application to increase the accessibility.
- Interconnection with institutional ERP systems of automated student data synchronization.
- Adoption of superior AI-powered face recognition so as to have a better authentication accuracy.
- Implementation of analytics and reporting dashboards in making decisions.
- Connectivity with smart campus technologies e.g. RFID gates or QR entry system.

## X. ACKNOWLEDGMENT

We would like to intimate our deepest gratitude to our project guide **Mr. Pratharv Surve**, Assistant Professor, Department of Information Technology, who assisted and always helped us to move through with the project. We have also used the services of the Department of Information Technology in **Thakur Shyammarayan Degree College**, Mumbai, which has been able to help us with the required academic support, and other required facilities to complete this work.

### *REFERENCES:*

- [1] NodeJS Documentation. Node.js JavaScript Runtime. On [nodejs.org/en/docs/](https://nodejs.org/en/docs/).
- [2] React Documentation. React- A JavaScript library to create the user interfaces. Available at <https://react.dev/>.
- [3] MongoDB Documentation. MongoDB Manual- NoSQL Database System. one can found at <https://docs.mongodb.com>.
- [4] Opencv Documentation. The Open Source Computer Vision Library. Retrieved in [opencv.org/docs/opencv](https://opencv.org/docs/opencv).
- [5] Python Software Foundation. Python Documentation. Meanwhile, available at the Python documentation site found at <https://docs.python.org/>.
- [6] OWASP Foundation. Web Application Security Guidelines. It can be found on <https://owasp.org/cmd-top-ten-www-project/>.

Smart Environments using Digital Identity and Access Management Systems. IEEE Xplore. Published on the internet at [ieeexplore](https://ieeexplore.org/).