INSE 6400 - Principles of Systems Engineering

Project Final Report - SMART CAMPUS

Submitted By	
Kunati Bala Krishna Yadav	40292128
Divya Varshini M	40293222
Gowri Annadurai	40292583
Venkata Sai Pavan Kumar Maniyambakam	40292946
Preetham Reddy Yerraguntla	40292244

Index

1. Introduction

Higher education stands as a fundamental right for students and plays a crucial role in contributing to a country's GDP. Students pursue higher education to gain knowledge and achieve their goals. However, the United States has witnessed alarming incidents of gun violence within and outside educational institutions in recent years. The University of Kentucky, for instance, has experienced instances where outsiders impersonated students, posing a serious threat to campus safety. These incidents are nightmarish for communities, resulting in the loss of lives and leaving students traumatised. It is imperative to prioritise student safety and implement stringent measures to protect them from potential harm. Additionally, many esteemed universities have grappled with cases of student impersonation during exams and classes, which undermines academic integrity and ethics. Therefore, there is an urgent need for Smart Campus initiatives that not only enhance student learning but also ensure their safety from life-threatening situations and uphold academic integrity to the highest standards.

In our project, Concordia University is chosen as our System and we will be investigating following areas in the context of campus security :

- Context Diagram
- Feasibility Analysis
- Operational Requirements
- Functional Analysis and Allocation

2. Potential need for the New System

In this phase, we will discuss about the problems within the Concordia University and the expected capabilities of new concept:

2.1 General Prospective

Security Concerns because of Campus being open to outsiders : This is very challenging aspect to distinguish students and staff from outsiders.

Impersonation : In university settings, such as during exams, on campus shuttle buses, and in libraries, impersonation poses serious concerns. Students may try to take examinations during exams for other people, which would be unethical.

Transportation : When shuttle buses are misused, other people outside the university can gain unlawful access to them to reach various locations or possibility of hijacking the shuttle buses as well.

Access to resources : In libraries, people can create fictitious identities to gain access to study materials or loan services and never return them.

The academic community's sense of justice and confidence is eroded by these acts, which calls for strict identity verification and security protocols.We suggest the use of Biometrics as

a comprehensive solution in response to the urgent need to protect student safety and maintain academic integrity in educational institutions.

By utilising biometric system , our suggested approach will transform academic integrity and campus safety. As a type of biometric security, for instance, facial recognition algorithms provide a strong layer of safety and authentication by reliably identifying people in real-time. Through the use of this technology, we hope to improve a number of elements within the educational ecosystem

2.2 New system requirements

Advanced recognition algorithms
Multi Factor authentication Access
High definition , Infra red , Wide angle Cameras
Turnstile gates ,
Database servers ,
User interface devices ,
Data Privacy, Storage and Retention Policies

2.3 Need Analysis :

Advanced Recognition Algorithms: These algorithms use machine learning to continuously improve accuracy by analyzing facial traits to accurately identify persons.

Multi-Factor Authentication Access: By demanding several forms of authentication, facial recognition improves security when combined with other factors like passwords or biometrics.

Wide-angle, infrared, and high definition cameras: These cameras are essential for precise facial recognition because they can capture sharp facial images in a variety of lighting situations.

Turnstile gates: Equipped with facial recognition technology, turnstile gates manage admission, permitting authorised people to move through while blocking unauthorised people from entering.

Database servers: Scalability, dependability, and data security are ensured by centrally located servers that safely store and handle facial recognition data.

User Interface Devices: To ensure seamless functioning, touchscreens or kiosks offer user-friendly points of interaction for enrolling, authenticating, or navigating facial recognition systems.

Data Privacy Policies : Since students biometric data will be stored, we have to come up with new policies related to data privacy, storage, retention and security, adhering to the laws of the Canadian Government .

2.4 Context Diagram

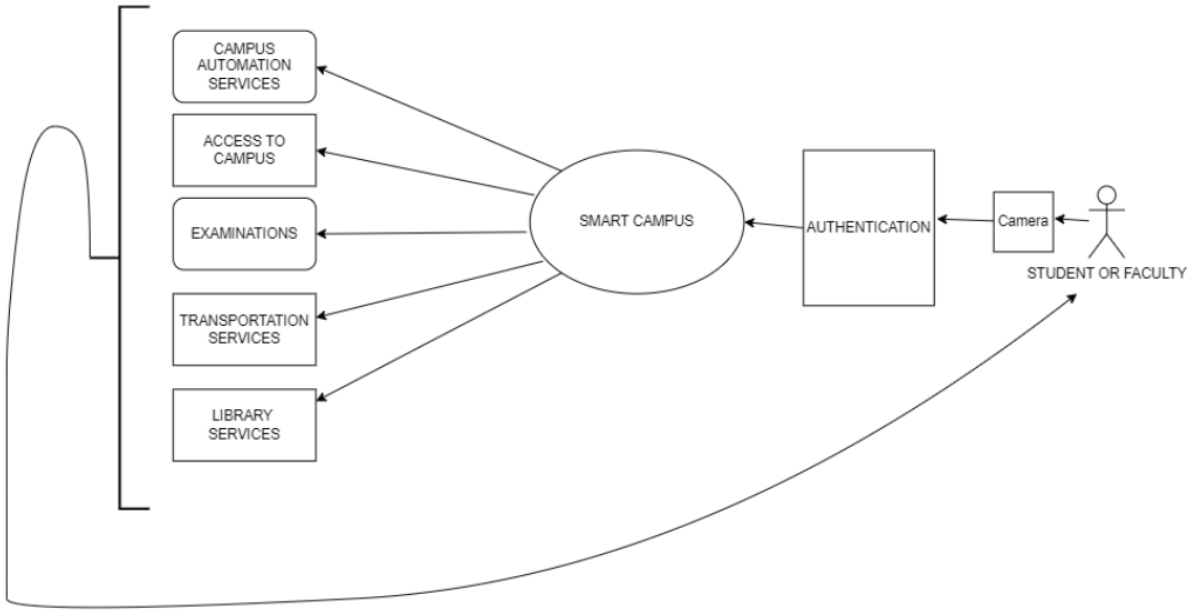

Figure 1 - Context Diagram

3. Generation of Alternatives :

For every problem in the real world scenario, we can find multiple solutions. We need to look into all of these possible solutions to compare and come to a final conclusion. In our case, for securing the campus, we have come across multiple technologies like Portable Fingerprint scanner, Turnstile Gates using RFID Technology , Attendance through student's Mobile device via Bluetooth connection, Face Recognition System etc., each with its own advantages and disadvantages.

Among these technologies Attendance through RFID technology and Attendance through Mobile Phone may give rise to the problem of fraudulent access, where, an unauthorised person may make use of the authorised student ID card or his mobile device and enter into the organisation. Hence, we haven't considered these technologies for our security requirement. Instead the other two alternatives that are considered for resolving this issue are :

1. Portable Fingerprint Scanner.
2. Automatic Face Recognition System

In the following section, an analysis will be conducted on both of these alternatives.

4. System Feasibility Analysis :

Feasibility Analysis is all about determining the practicality or possibility of bringing the project we are working on into reality and whenever a new system or concept is proposed, it is always necessary to illustrate the feasibility of that particular system. The following

sections provides a detailed analysis on the operational feasibility, technical feasibility, schedule feasibility and economic feasibility for the above mentioned systems :

4.1 Operational Feasibility

The Operational Feasibility of this project is centred around analysing the strengths and weaknesses of this Attendance Marking System and requires a comprehensive approach to address various factors. Regulatory Alignment and Compliance are one of such key factors, as we are working with sensitive data of the students. This requires an in depth understanding of the current laws related to data privacy, security and retention policies in Canada.
Simultaneously, we have to focus on technological integration as well, considering the latest developments in the field of AI and Deep Learning Technologies. The chosen technology should be able to detect or analyse the biometrics with utmost accuracy in all times of the day and should be independent of the exposure to light or other factors.To ensure these, we have used a standard SWOT analysis technique comparing the pros and cons of both the proposed alternatives for better decision making.

4.1.1 SWOT Analysis : Portable Fingerprint Scanner vs. Automatic Face Recognition System

- Strengths
  - Portable Fingerprint Scanner:
    - It provides highly accurate and reliable identification based on unique fingerprint patterns.
    - Compact and portable design for easy deployment and convenience.
    - Resistant to environmental factors like sunlight or exposure.
    - It is an established technology with widespread adoption and user base.
  - Automatic Face Recognition System:
    - It is a contactless and non-intrusive identification process
    - Has the ability to identify individuals from a far distance and in a short period of time.
    - Has the potential for integrating with existing surveillance or security systems.
    - Has better scope as it can leverage the advancements in computer vision and deep learning technologies.
- Weaknesses
  - Portable Fingerprint Scanner:
    - Requires physical contact with the sensor, which might not be convenient for everyone.
    - Can raise potential hygiene concerns, especially in the context of viral diseases like COVID-19.
    - Fingerprint scanning can be affected by finger injuries or even by environmental conditions like temperature and humidity.
    - It is a very slow and manual process as each person has to scan their fingerprints one after the other.

        - They are now an outdated technology and there has been many cases of tampering the fingerprints by making use of wax or resin.
    - Automatic Face Recognition System:
        - Accuracy can be influenced by factors like lightning and changes in facial appearances.
        - It can raise potential privacy concerns and ethical considerations around the usage of the stored biometric data.
        - Its initial investment is high considering the latest hardwares and softwares.
- Opportunities
    - Portable Fingerprint Scanner:
        - Widespread adoption in access control, attendance and financial transactions.
        - Increasing demand for reliable and secure identification solutions.
        - It has the potential for integrating with other biometric modules for enhanced security.
    - Automatic Face Recognition System:
        - Growing demand for contactless and automated identification systems, especially in the post-pandemic era.
        - Accuracy and Reliability of these systems increases with the advancements in deep learning and computer vision techniques.
        - It has the potential for integrating with existing surveillance or security infrastructure.
- Threats
    - Portable Fingerprint Scanner:
        - Competition from alternative advanced biometric technologies like facial recognition and iris scanning
        - Concerns about data privacy and security of the fingerprint data
        - Possibility for spoofing the fingerprints using artificial fingerprints or gummy bears.
    - Automatic Face Recognition System:
        - One major threat is with the regulatory and ethical concerns around the usage of facial recognition technology leading to potential restrictions or bans.
        - Competition from alternative advanced biometric technologies like iris scanning and voice recognition.
        - Scope for adversarial attacks and techniques to bypass the facial recognition systems.

In conclusion, both the portable fingerprint scanner and the automatic face recognition systems have their own strengths and weaknesses. The choice between the two technologies will depend on the specific requirements of the application, the desired level of security, user preferences etc., Hence, we will be proceeding further with other feasibility analysis to make a better decision.

4.2 Technical Feasibility: Portable Fingerprint Scanner vs. Automatic Face Recognition System

To compare the technical feasibility of the portable fingerprint scanner and the automatic face recognition system, we have used a weighted decision matrix with 5-point scale. The key factors that are considered are :

- Hardware Compatibility : It is the ability of the system to integrate with the required hardware components like cameras, sensors, processors, etc., and should be given a higher weightage.
- Software Capabilities : It is the sophistication and robustness of the software algorithms and infrastructure required for the functioning of the biometric system. This should also be given priority as that of the Hardware Compatibility.
- Scalability : It is the system's ability to handle increasing users count and data without a significant degradation in its performance.
- Reliability : The consistency and accuracy of the biometric system, even in challenging conditions.
- Integration Complexity : The ease of integrating the biometric system with the existing IT infrastructure and applications.

The weighted decision matrix is as follows :

Criteria	Weight	Portable Fingerprint Scanner	Automatic Face Recognition System
Hardware Compatibility	0.25	4	4
Software Capabilities	0.25	4	5
Scalability	0.15	4	5
Reliability	0.20	3	5
Integration Complexity	0.15	4	3
Total Weighted Score	1.00	3.80	4.30

Table 1 - Weighted Decision Matrix

The weighted decision matrix shows that the automatic face recognition system has a slightly higher total weighted score(4.30) compared to that of the portable fingerprint scanner(3.80). This indicates that, although the facial recognition system has slightly higher integration complexity, overall, the face recognition system is more technically feasible compared to the portable fingerprint scanner.

4.3 Schedule Feasibility:

Portable Fingerprint Scanner

- It has a relatively straightforward implementation process.

- Hardware and software integration with existing systems can be completed in a shorter timeframe.
- Its a mature technology with well-established deployment practices and support from vendors

Automatic Face Recognition System

- It requires a more complex implementation process, including hardware procurement, software development and its integration.
- It requires a longer timeframe for designing, testing and deploying the system. especially if custom algorithms or infrastructure are required.
- There is a potential need for technical expertise and resources for ensuring its optimal functioning.

While the portable fingerprint scanner can be implemented more quickly due to its simplicity and simpler integration requirements, the automatic face recognition system may require a longer timeline to ensure a comprehensive and robust solution. However, the increased technical capabilities and versatility of the face recognition system can justify the longer implementation period, especially in the world of continuous advancements in the field of computer vision and deep learning technologies, with increased performance, reliability and security.

4.4 Economic Feasibility:

Note : Since, fingerprint scanning is a manual process and can consume a lot of time, if scanning is done one by one using a single device alone. To speed up this attendance marking process, we are assuming that, we will be maintaining at least 5 or more fingerprint scanners for an ideal class of 60 to 100 students.

Economic Feasibility	Automatic Face Recognition System	Portable Fingerprint Scanner
Hardware and Equipment	Requires fewer hardware components, primarily cameras	The costs include purchasing multiple devices for each classroom
Software	It may include purchasing or developing the face recognition algorithms	It may involve purchasing software licenses for each device
Training	Training may be necessary for system administrators and faculty on enrollment and usage procedures	Minimal to no training is required for users to operate the devices
Maintenance	Generally has lower maintenance costs as it relies on fewer physical components. Maintenance may involve software updates, system monitoring, and occasional hardware checks	Requires regular maintenance, including calibration, cleaning and potential repairs for multiple devices.
Scalability	Generally more scalable as it can handle larger groups with minimal additional hardware investment.	Scaling up the attendance system to accommodate larger groups requires purchasing additional devices, which can lead to a significant upfront costs

Developer Costs	Requires skilled developer to implement and maintain the system	Less need for hiring developers as it is already an existing and readily available technology
Cost of not implementing the Security Feature	Campus becomes less secure as outsiders can easily enter the classrooms, without any authentication. Students might involve in malpractices and proxy during the attendance, which might not be in the best interests of the student's future and the reputation of the university.	

Table 2 - Economic Feasibility

Considering the factors mentioned above, the automatic face recognition system is more economically feasible in the long run perspective.While it may require higher initial investment in software development and hardware setup, it offers cost savings in terms of hardware, maintenance and user training compared to that of deploying multiple portable fingerprint sensors. Additionally, the accuracy and efficiency of face recognition systems justify the investment, especially in scenarios where maintaining class discipline, attendance accuracy and security are crucial.

5. Trade – off analysis

Tradeoff analysis is a critical phase that furnishes crucial information to facilitate the decision-making process. It encompasses four pivotal steps.

The initial step involves identifying the shortcomings within the system, defining objectives, and assessing the system's effectiveness based on each criterion.

The subsequent step entails identifying alternative solutions capable of addressing potential drawbacks within the system while meeting the specified requirements.

Thirdly, the evaluation phase focuses on assessing the efficiency, feasibility, risk, and cost of each alternative, employing interpretative and statistical methodologies. Analytical models and experiments are utilized to generate estimated measures of effectiveness.

Furthermore, a comprehensive comparison of the alternatives is conducted based on various factors.

Lastly, the optimal alternative is selected based on predefined criteria and preferences.

		Face Recognition		**Fingerprint Scanner**	
Criteria	**Weight**	V	W*V	**V**	W*V
Accuracy	**20%**	4	0.8	5	1
Security	**20%**	4	0.8	2	0.4
User Convenience	**10%**	3	0.3	2	0.2

Cost	**15%**	3	0.45	4	0.6
Speed	**20%**	5	1	2	0.4
Environmental Impact	**5%**	4	0.2	4	0.2
Ease of Setup	**5%**	2	0.1	1	0.05
Privacy Concerns	**5%**	3	0.15	3	0.15
Cost		$100		$80	
Weighted Sum		**3.8**		**3**	
Weighted Sum/Cost		**0.0380**		**0.0375**	

Table 3 - Trade-off Analysis

According to the defined requirements and feasibility analysis, it is clearly a best decision to choose Facial Recognition System over Fingerprint Scanners.The first alternative was chosen based on the accuracy, security and speed of the authentication system. However the second alternative, would have been the best, if cost is alone considered as a priority.

6. System Operational Requirements

The operational requirements define the means by which the teachers and students needs will be fulfilled by the smart campus system. It describes the key features, performance characteristics, and operation of the system. This covers the system's use by instructors and students as well as its interactions with other systems. In summary, it explains the functionality of the smart campus system in a form that is simple for users to comprehend.

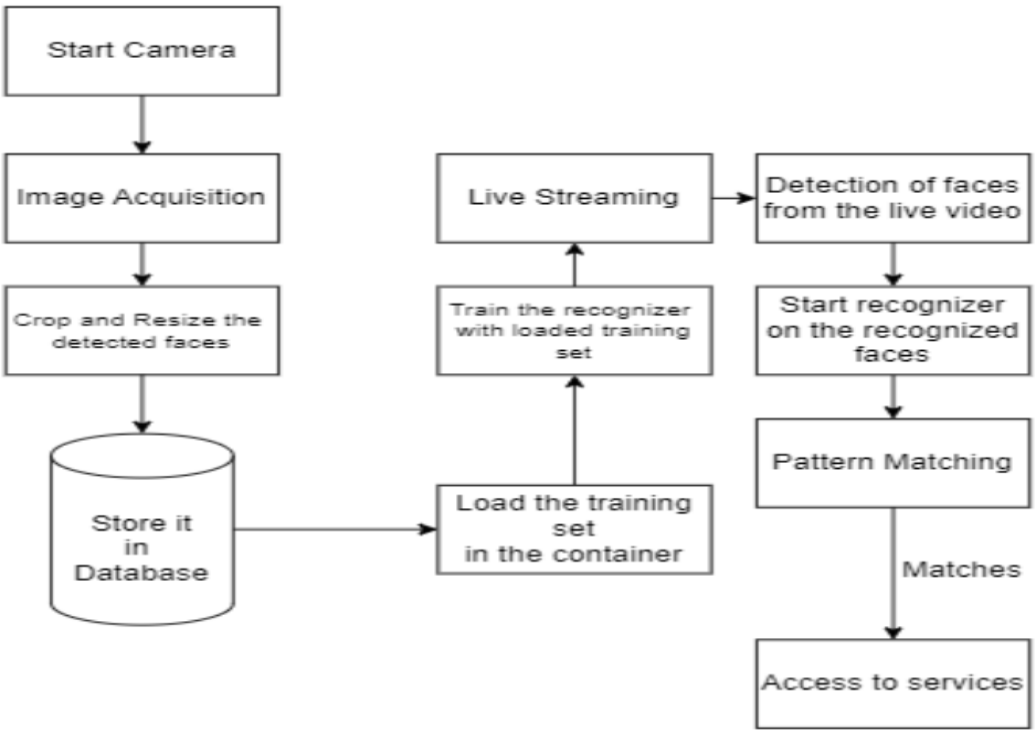

Figure 2 - System Operational Requirements

Students can be pictured from various perspectives and stances using a live camera. The next step in processing these photos is to isolate certain interest regions, which will aid in identifying the pupils. The photos are cropped, then resized to a normal size and turned into grayscale. Ultimately, the edited photos are stored in a folder with the pupils' names on it.

We use OpenCV with the Haar-Cascade Classifier approach to detect faces. This method must be trained to recognize particular features before it can correctly identify faces. We call this method feature extraction. In our example, we trained the Haar cascade algorithm to detect frontal human faces using an XML file named "Facial_recognition_system".

The face recognition process involves three main steps: preparing training data, training the face recognizer, and making predictions. Initially, the dataset consists of photos of students, each associated with a unique label. These photos are then used to train the face recognizer. In this system, the Local Binary Pattern Histogram method is utilised for face recognition.

During training, the Local Binary Patterns (LBPs) for each face in the dataset are compiled and transformed into decimal numbers. Histograms are then created based on these decimal values, representing the distribution of features within each image. Essentially, each image in the training data is represented by its own histogram.

When it comes to recognition, the histogram of the face to be identified is generated and compared against the histograms of the previously trained faces. The system then

determines the best-matched label associated with the student, allowing for accurate recognition.

6.1 Defined System Operational Requirement

- Educational Technology System:

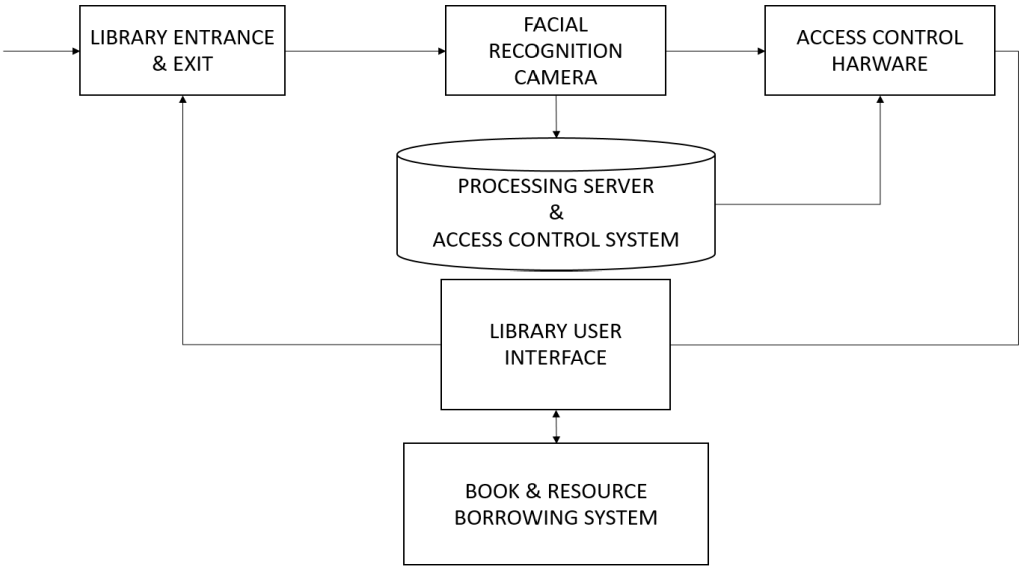

Figure 3 - Library System

1. Library Entrance & Exit:
    - Entrance and exit to the library.
2. Facial Recognition Camera:
    - High definition camera to capture the picture of the entered individual.
    - Connected to both server and the access control hardware.
3. Processing Server & Access Control System:
    - Image from the camera is fed as an input and checked whether the individual is present in the database.
    - A decision is made by the system and the command to grant access or not is sent to access control hardware.
4. Access Control Hardware:
    - Command is received from the control system whether to grant access to the individual or not.
5. Library User Interface:
    - Individuals make use of this interface to interact with the borrowing system.
6. Book & Resource Borrowing System:
    - The system contains algorithms to seamlessly perform the book or resource borrowing process.
    - Takes an individual's Id to store the data necessary for the borrowing and returning of the book or resource.

- Campus Safety and Security Systems:

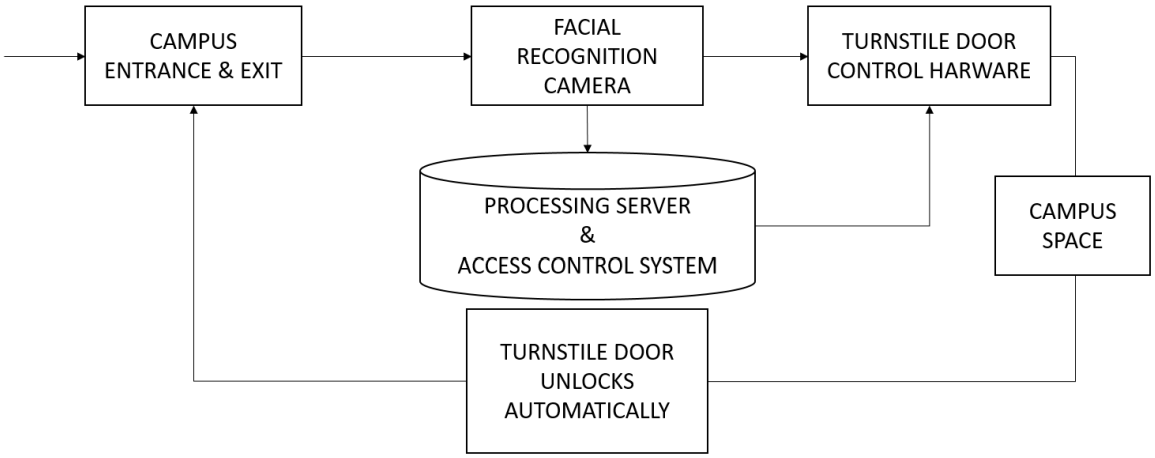

Figure 4 - Campus Security System

1. Campus Entrance & Exit:
    - Entrance and exit to the Campus.
2. Facial Recognition Camera:
    - High definition camera to capture the picture of the entered individual.
    - Connected to both server and the control hardware.
3. Processing Server & Access Control System:
    - Image from the camera is fed as an input and checked whether the individual is present in the database.
    - A decision is made by the system and the command to grant access or not is sent to control hardware.
4. Turnstile Door Control Hardware:
    - Command is received from the control system whether to grant access to the individual or not.
5. Campus space.
6. Turnstile Door Unlocks Automatically:
    - Automatic unlocking of the turnstile doors whenever an individual is trying to exit.
    - The presence of an individual is sensed by the motion sensor.

- Building Automation System:

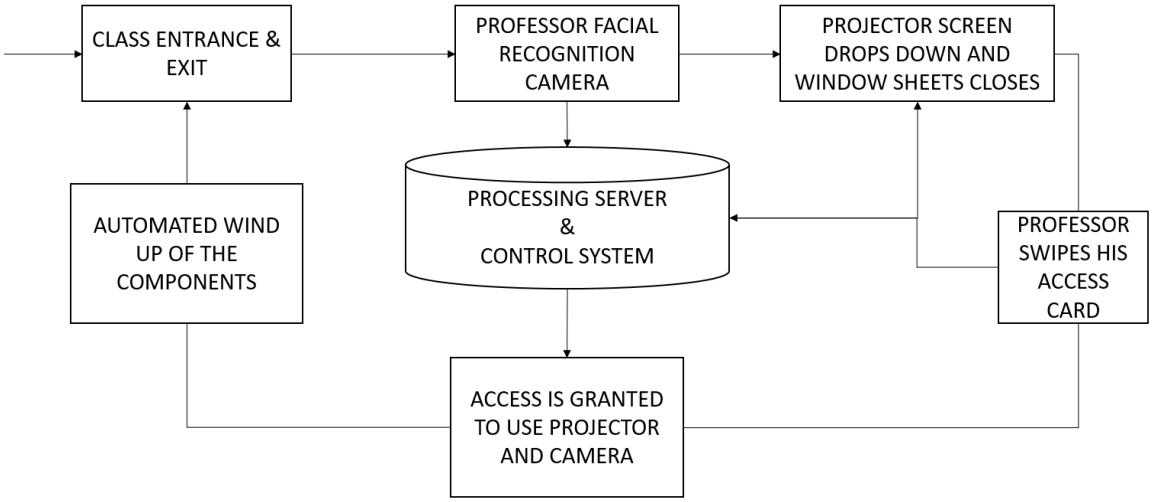

Figure 5 - Automation System

1. Class Entrance & Exit:
    - Entrance and exit to the Class.
2. Professor Facial Recognition Camera:
    - High definition camera to capture the picture of the entered individual.
    - Connected to both server and the screen and window sheets control hardware.
3. Processing Server & Control System:
    - Image from the camera is fed as an input and checked whether the individual is present in the database.
    - A decision is made by the system and the command to drop down the projector screen and closing of window sheets is sent to control hardware.
4. Access card swiping:
    - Professor swipes their respective access cards and a command is sent.
5. Projector and Camera:
    - If the command to access is granted, the professor is allowed to use the projector for lecture and camera can be used for recording the lecture hour.
6. Automated wind up of the components:
    - As soon as the class is completed the system automatically shuts down and all the components are wound up.

- Smart Transportation System:

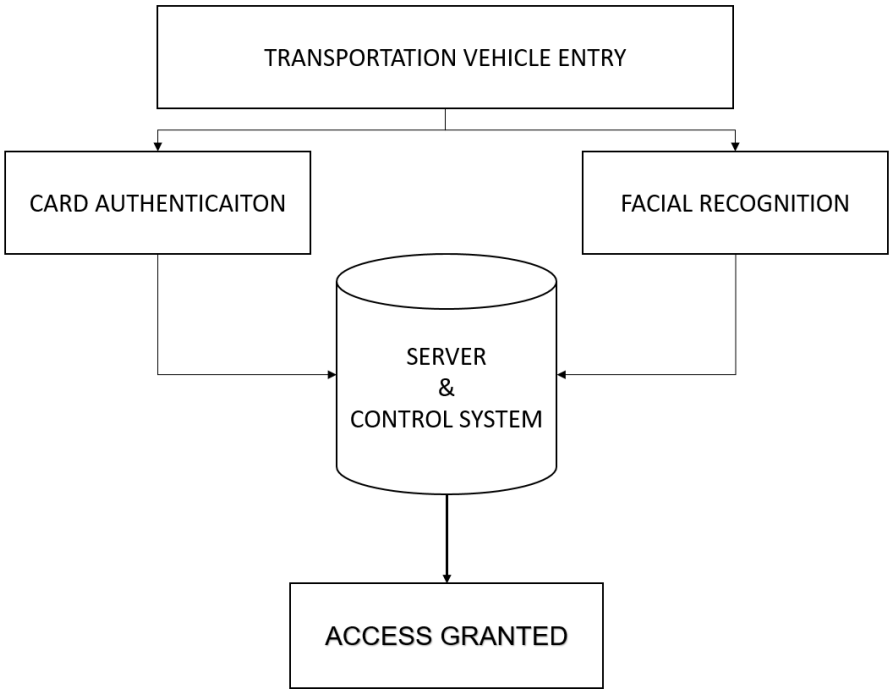

Figure 6 - Transportation System

1. Transportation Vehicle Entry:
    - Students enter the vehicle through this entry.
2. Card Authentication:
    - Students swipe their Access card for entry.
    - This data is passed on to the Server & Control system for further process.
3. Facial Recognition:
    - Picture of the student's face is captured.
    - This is sent as an input to the Server & Control system for further process.
4. Server and Control System:
    - Both the inputs form the card authentication and the camera is taken and checked whether they are matching and also present in the institution database.
    - A decision is displayed.
5. Access Granted:
    - If the decision displayed is “Access Granted”, the individual is good to seat in the vehicle, if not, the individual is kindly asked to leave and check with the management.

- Information and Communication System:

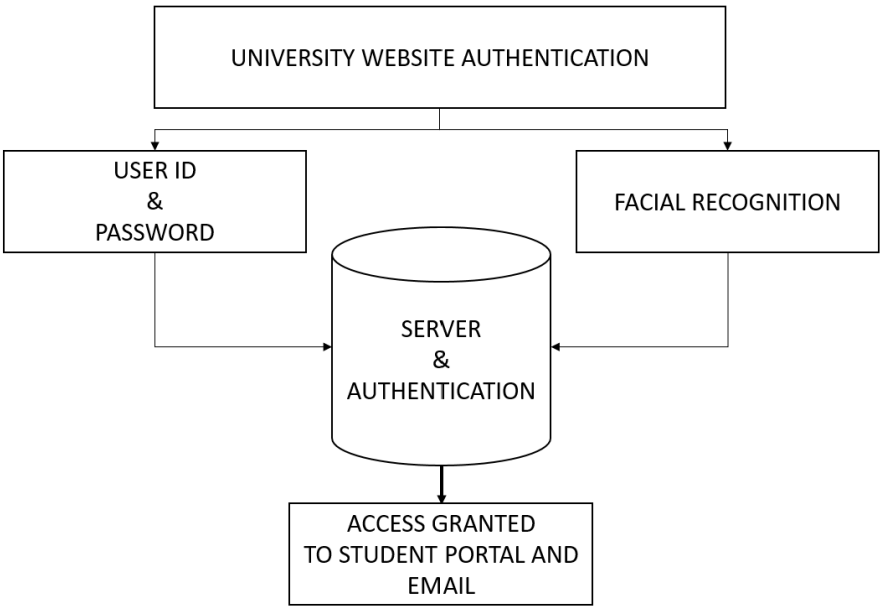

Figure 7 - Information and Communication System

1. University Website Authentication:
    - Students open the main page of the university website and select the student portal or university mail.
2. User ID & Password:
    - Students enter their login credentials.
    - This data is passed on to the Server & Authentication for further process.
3. Facial Recognition:
    - Picture of the student's face is captured.
    - This is sent as an input to the Server & Authentication for further process.
4. Server and Authentication:
    - Both the inputs from the login page and the camera are taken and checked whether they are matching and also present in the institution database.
    - A decision is made.
5. Access Granted:
    - Once they are checked and access is granted the student is good to use the student portal or University mail, if not, the student is kindly asked to check with the IT services.

7. Functional analysis and allocation

Functional Analysis and Allocation is a top-down process of translating system level requirements of the Automatic Face Recognition System into detailed functional and performance design criteria.

7.1 System Functional Breakdown

Class Function	Element Function	Component
Signal : Includes all the components responsible for capturing, preprocessing and extracting the necessary facial data from the input.	Receive Signal Process Signal	Image Capture - Pre Processing - Face Detection Algorithms - Feature Extraction - Face Recognition
Data : Includes analysis, interpretation, organization and conversion of the data	Input Data, Process Data, Output Data	Database of Encodings - Compare input data with Database - Match Found or Not Found - Backup Data - Attendance Records and Reports
Material : Defines the physical hardware components required for the system	Computer Hardware, Software, Network Hardware	Camera Hardware (lenses, sensors, etc.,) - Processing Unit - Storage Devices - Servers
Energy : The energy resources needed for the system to function	Electricity	Power Supply - Backup Power Sources for uninterrupted operation

Table 4 - Functional Breakdown

7.2 Functional Analysis

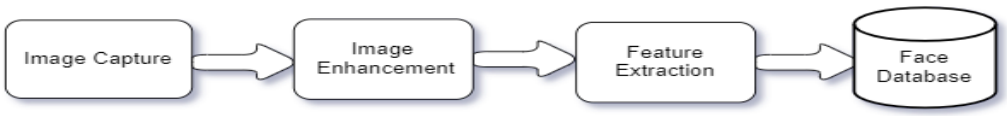

Figure 8 - Enrollment Process of a Student

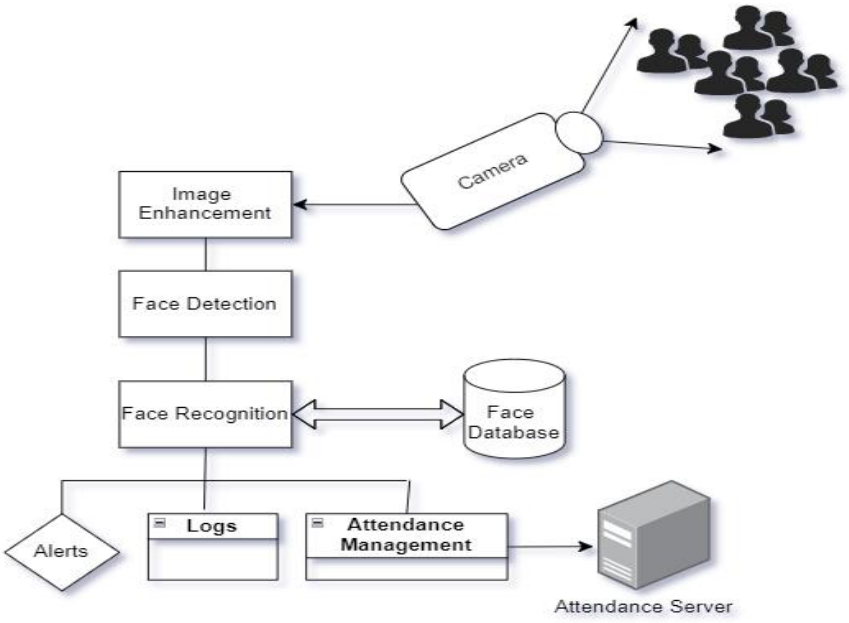

Figure 9 - Functional Block Diagram for Automatic Face Detection System

8. Conclusion

In conclusion, we have meticulously explored various methodologies for implementing a smart campus infrastructure. Each alternative had its own advantages and disadvantages. However, after thorough evaluation, it is evident that Biometric Systems, particularly Portable Fingerprint Scanners and Facial Recognition Systems, form the most promising solutions among the other considered alternatives.

Having conducted a detailed feasibility analysis on both these solutions, we confidently assert that Facial Recognition Systems provide the best fit for our classrooms. They strike the right balance between being effective and fitting in with what we need.Their advanced capabilities coupled with their adaptability to our specific needs, position them as the preferred choice for the Smart Campus System. By implementing these Facial Recognition Systems, we can seamlessly integrate the cutting-edge technologies into our educational environment, thereby enhancing security, efficiency and overall student experience.

9. Tables and Figures :

10. References :

[1] https://www.tsa.gov/news/press/factsheets/facial-recognition-technology

[2] https://www.irjmets.com/uploadedfiles/paper//issue_5_may_2022/23543/final/fin_irjmets1652991544.pdf

[3] https://www.sciencedirect.com/science/article/pii/S1877050921019232

[4] https://blogs.illinois.edu/view/9099/1559685706

[5] https://www.ellucian.com/emea-ap/blog/facial-recognition-can-give-students-better-service-and-security

[6] https://www.unesco.org/en/higher-education/need-know