MINOR-2 PROJECT

END TERM REPORT

For

SaaS for secured access of events

Submitted By:

Name	**SAP ID**	**Specialization**
Raja Kunal Pandit	500085839	CCVT
Vikrant Singh	500083599	CCVT
Vikrant Kaushik	500083739	CCVT
Harshit Krishna	500084907	CCVT

Department of Systemics
School Of Computer Science
UNIVERSITY OF PETROLEUM & ENERGY STUDIES,
DEHRADUN- 248007. Uttarakhand

Ms. Avita Katal
Project Guide

Dr. Neelu J. Ahuja
Cluster Head

Under the guidance of

Avita Katal
Assistant Professor (SS)
SCHOOL OF COMPUTER SCIENCE
University of Petroleum and Energy Studies

Project Title

Saas for secured access to events.

Abstract

The proposed project aims to develop an access control system for events on a campus. The system will utilize digital identities, such as QR codes to link an individual's identity to the event. Every individual will have their own unique QR code. By scanning the digital ticket at the event, the system will be able to verify the individual's identity and grant access to the event. If the person's identity mismatches then the application will notify the threat to the event organizers. This will ensure that only authorized individuals are able to enter the event, preventing unauthorized access and enhancing security for the campus community. The system will be easy to use and will be a cost-effective solution for managing access to events on campus , college , hotels, party organizations etc. The project has a very wide range of application scope .

ACKNOWLEDGEMENT

We wish to express our deep gratitude to our mentor Asst. Prof. Avita Katal, for all advice, encouragement, and constant support he has given us throughout our project work. This work would not have been possible without his support and valuable suggestions.

We sincerely thank our cluster head, Prof. (Dr.) Neelu J. Ahuja, for her great support in doing our project at SoCS.

We are also grateful to Dr. Ravi S. Iyer Dean, SoCS, UPES for giving us the necessary facilities to carry out our project work successfully.

We would like to thank all faculties from UPES for their help and constructive criticism during our project work. Finally, we have no words to express our sincere gratitude to our parents who have shown us this world and for every support they have given us.

TABLE OF CONTENTS

Sr. No.	Contents	Page No.
1.	Introduction	4
2.	Literature Review	4
3.	Problem Statement	5
4.	Objective	5
5.	Methodology	6
6.	Area of application	7
7.	SDLC	7
8.	Implementation and result	8-13
9.	SWOT Analysis	14
10.	PERT Chart	15
11.	References	16

1. Introduction

In this era of rapidly increasing technology, every system needs to be fast, secured and highly efficient. So, this project focuses on smoothening the work of event management professionals as well as for any campus event systems. This project will allow event organizers to create events, form creation, collect attendee data and generate data sheets, and store all the entities in a secure database.

The system will use the stored data to generate a unique QR code for each attendee. The QR code will be generated by encrypting the attendee information using a hash function which will enhance the security measures. This encrypted information will be used to generate a QR code, which will be sent to each attendee. The QR code will serve as a secure and efficient entry pass to the event. This project work would be in a web application format connected with a database with enhanced security features. There will be proper implementation and integration of microservices so that the solution would be scalable and user-friendly for both event organizers and attendees.

2. Literature Review

This project focuses on smoothening the work of event management professionals as well as for any event management systems. The project comprises a lot of different functionalities and modules. Set of different modules and microservices make the project fault tolerant , flexible and much more secure.It proposes a lightweight authentication system with the concept of QR codes. The system aims to provide a secure and convenient authentication process for mobile users.[1] The authors propose a QR code-based authentication scheme that uses a secret key to generate a QR code on a server. The QR code is then scanned by the user's mobile device to authenticate the user and complete the login process. The authors evaluate the proposed system in terms of its security, efficiency, and usability, and conclude that the QR code-based authentication system is a promising solution for mobile devices.The paper[2], concludes that the system is effective in providing secure online transactions, as it offers a simple and convenient way for users to authenticate their transactions without the need for cumbersome passwords or traditional security tokens.[6]. The problem with QR codes is that there is a lack of awareness among the corporate world about people interested in developing and using QR code. QR code based authentication is beneficial to users, cost effective and less time consuming. [7] Micro services are popular as they offer a new paradigm and many benefits such as flexibility, scalability, ease of development and manageability of applications. The concept of microservices is implemented so as to make the application resilient , secured , scalable and fault tolerant.

3. Problem Statement

There is always a lack of a centralized and secure system for managing access to events . There is a need for a solution that can efficiently control who is granted access to events, ensure that only authorized individuals are able to attend, and provide an organized and auditable system for managing event attendance. The solution must be scalable and user-friendly for both event organizers and attendees, and should be able to integrate with existing campus systems such as identification systems and event scheduling tools. Implementing the microservice architecture in the system to obtain a resilient , secured , scalable and fault tolerant system is still a hurdle to pass.

4. Objectives

- To implement the access control for events and make a centralized and secured system .
- To understand and implement the concepts of Object Oriented Programming and databases.
- To understand the cryptography techniques.
- To understand and implement the different phases of SDLC.

5. Methodology

For this project, firstly taking the list of attendee of an event as an input having the details Name, email id and contact number. Then storing the data in the database having the details of attendee and also the status whether the particular person has entered in the event or not. Now generating the unique QR code for each attendee, after generating QR code sending it to each attendee which will be used as entry paas. At the time of entry, the digital entry pass is scanned which is in the QR code format. After scanning , the encrypted attendee information is fetched as a hash value.

The hash value is compared with the system database and if the encrypted hash value matches then the permission is granted else the threat is notified to the organization's system. This will ensure that only authorized individuals are able to enter the event, preventing unauthorized access and enhancing security for the campus community. The concept of microservices is implemented so as to make the application resilient , secured, scalable and fault tolerant.

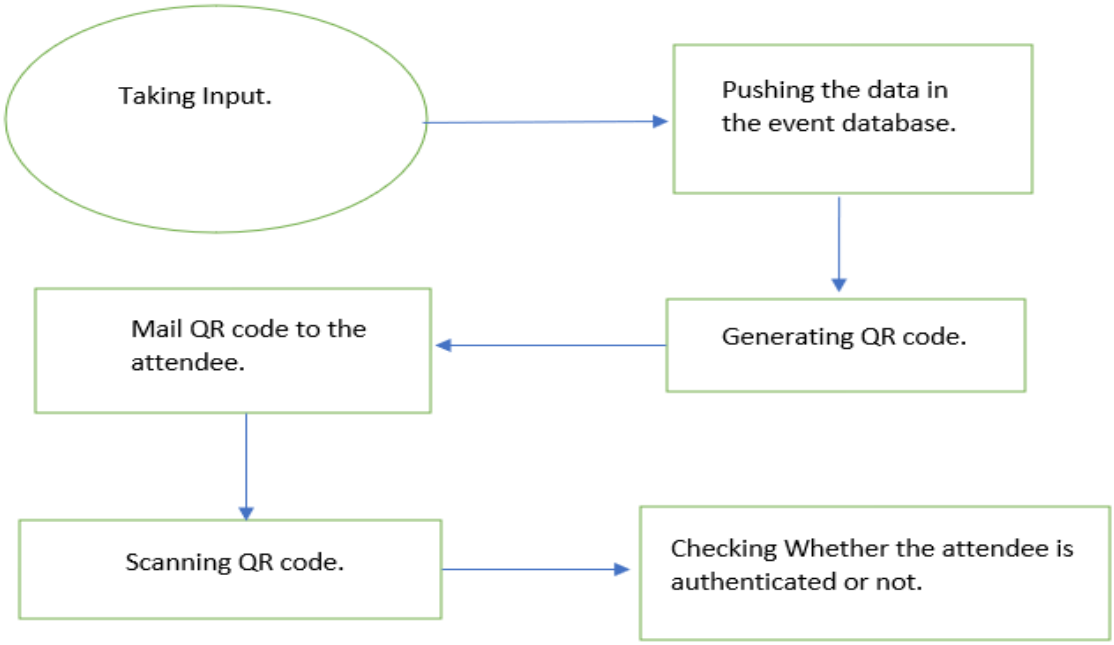


Fig 1: Flowchart

6. Area Of Application

- Event Access Control: The SaaS can be used to secure access to events by using QR codes and cryptography to verify the identity of attendees.

- Attendee Tracking: The SaaS can track the attendance of attendees using MongoDB and QR codes, providing a secure and efficient way to keep a record of who attended an event.

- Data Security: The SaaS can ensure the security of sensitive event-related information stored in MongoDB through the use of cryptography.

- Event Planning and Management: The SaaS can be used to plan and manage events, from scheduling to communication with attendees, in a secure and efficient manner.

- Marketing and Analytics: The SaaS can be used to analyze event attendance and feedback to improve event planning and marketing efforts.

7. SOFTWARE DEVELOPMENT LIFE CYCLE

In this project, we are approaching the Agile model to avoid the complexity of our project. This Agile method works upon the principle of SDLC (Software Development Life Cycle).Here, we are developing our project by keeping the criteria of the Agile model in our mind. The methods which we are using are as follows:-

Collaborative decision-making: It is a process that is collaborative, iterative, and transparent. It means all stakeholders are updated on assigned tasks at regular intervals, they give feedback, and then the team knows what needs to be changed or improved.

Small modules: This suggests that the model we are working on won't be completed in a single phase. Small modules of a whole model will be implemented step by step.

Testing: Here testing occurs in two phases:-

- ❖ Unit testing: This testing is done at the completion of each module to avoid a large number of errors in a model.
- ❖ Integrated testing: This testing will be done at the end of model development to check whether the desired output has been procured or not.

8. Implementation and result:

Creating qr code to respective user

```python
import qrcode
import io

def create_qr_code(data):
    # Creating an instance of QRCode class
    qr = qrcode.QRCode(version = 1,box_size = 5,border = 5)
    # Adding data to the instance 'qr'
    qr.add_data(data)
    qr.make(fit = True)
    img = qr.make_image(fill_color = 'red', back_color = 'white')
    # Save the image to a binary stream
    stream = io.BytesIO()
    img.save(stream)
    # Reset the stream position to the beginning
    stream.seek(0)
    print("qr Created successfully")
    return stream
```

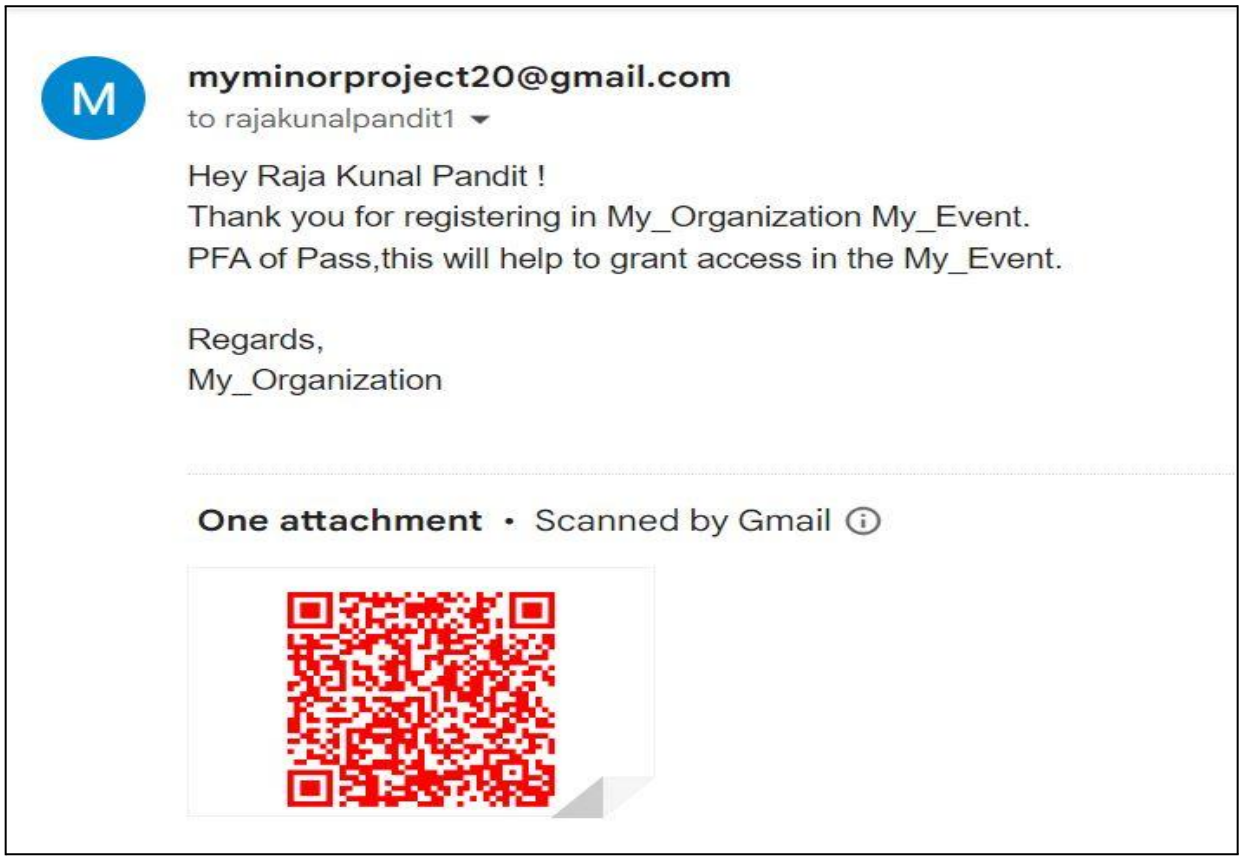
Sending mail to users:

```python
def sendMail(email_sender, email_password, email_receiver, subject, body, binary_image_data):
    en=EmailMessage()
    en['From']=email_sender
    en['To']=email_receiver
    en['Subject']=subject

    en.set_content(body)

    # Create a BytesIO object from the binary image data
    image_stream = BytesIO(binary_image_data)
    # Create an Image object from the binary data
    image = Image.open(image_stream)
    # Save the image to the BytesIO object
    image.save(image_stream, format='PNG')
    # Reset the stream position to the beginning
    image_stream.seek(0)
    # Add the image data to the email attachment
    en.add_attachment(image_stream.read(), maintype='image', subtype='png', filename='qrcode.png')
    context=ssl.create_default_context()

    with smtplib.SMTP_SSL("smtp.gmail.com", 465, context=context) as smtp:
        try:
            smtp.login(email_sender, email_password)
            smtp.sendmail(email_sender, email_receiver, en.as_string())
            print("Email sent successfully.")
        except Exception as e:
            print("An error occurred while sending the email:", e)
```

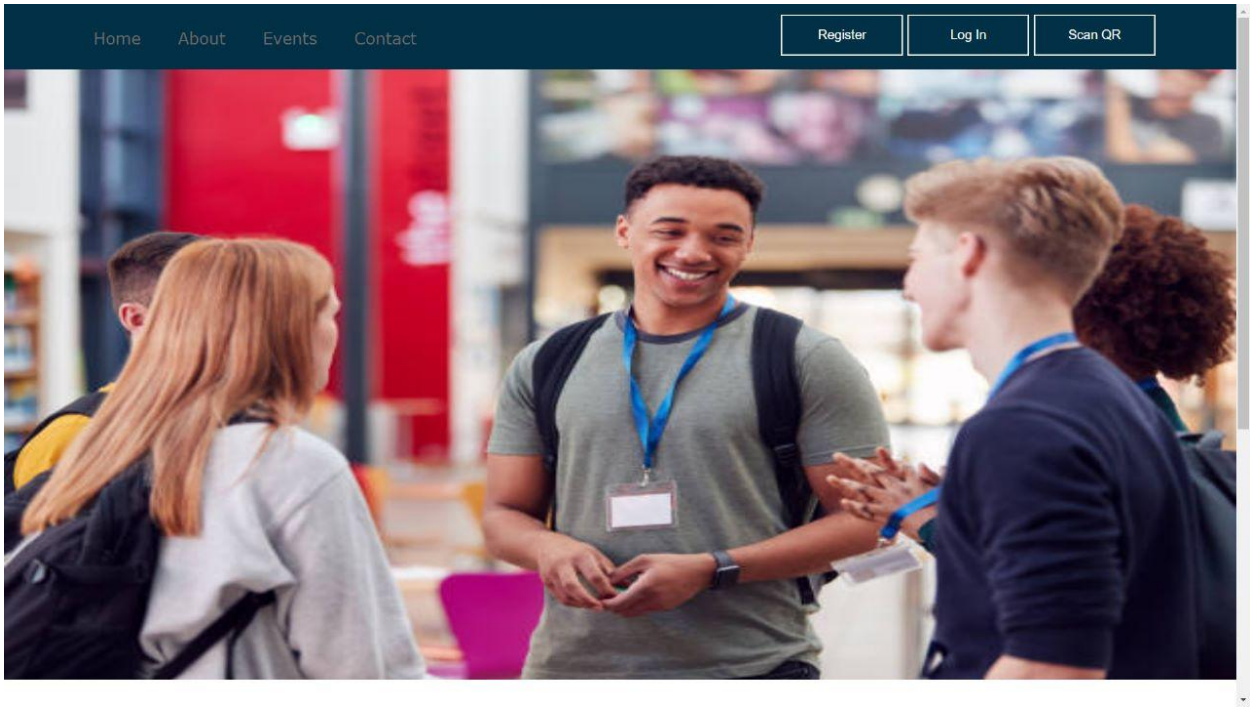
Encrypt/Decrypt users details before generating QR:

```python
def encrypt_message(message, key):
    backend = default_backend()
    padder = PKCS7(128).padder()
    message = padder.update(message.encode()) + padder.finalize()
    cipher = Cipher(algorithms.AES(key), modes.ECB(), backend=backend)
    encryptor = cipher.encryptor()
    ct = encryptor.update(message) + encryptor.finalize()
    return ct

def decrypt_message(ciphertext, key):
    backend = default_backend()
    cipher = Cipher(algorithms.AES(key), modes.ECB(), backend=backend)
    decryptor = cipher.decryptor()
    message = decryptor.update(ciphertext) + decryptor.finalize()
    unpadder = PKCS7(128).unpadder()
    message = unpadder.update(message) + unpadder.finalize()
    return message.decode()
```

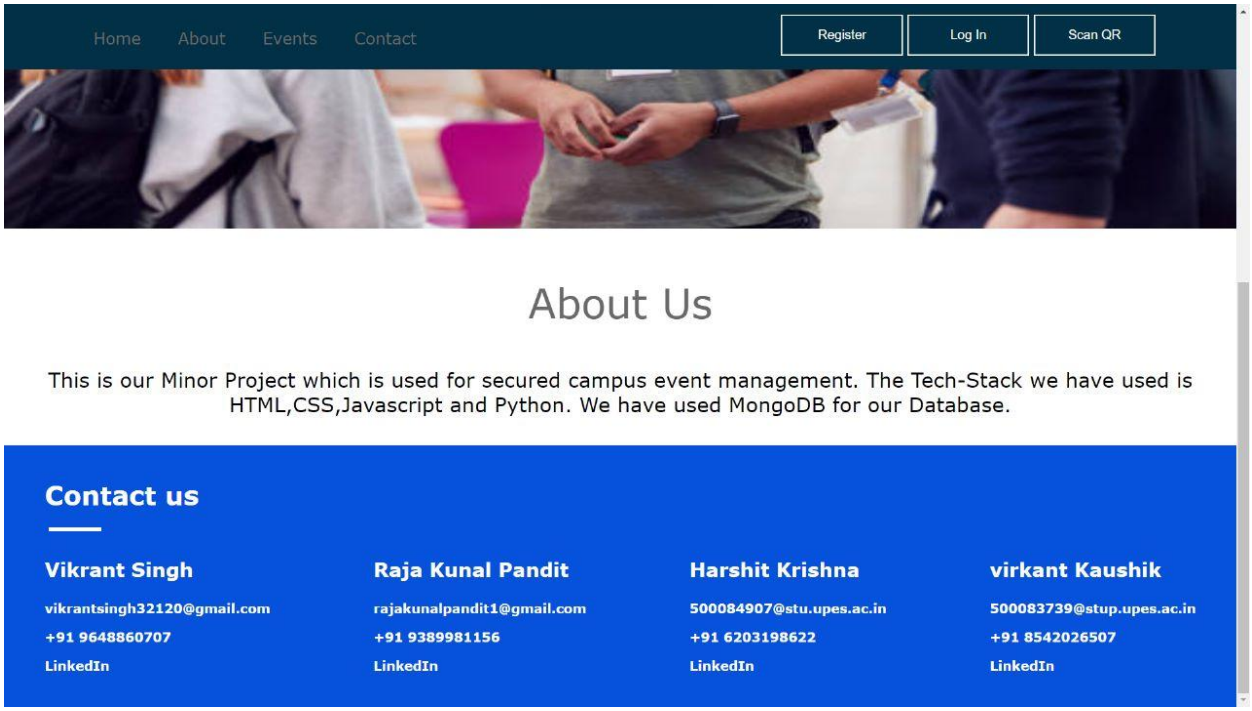
Sample Mail Received to Respective users:



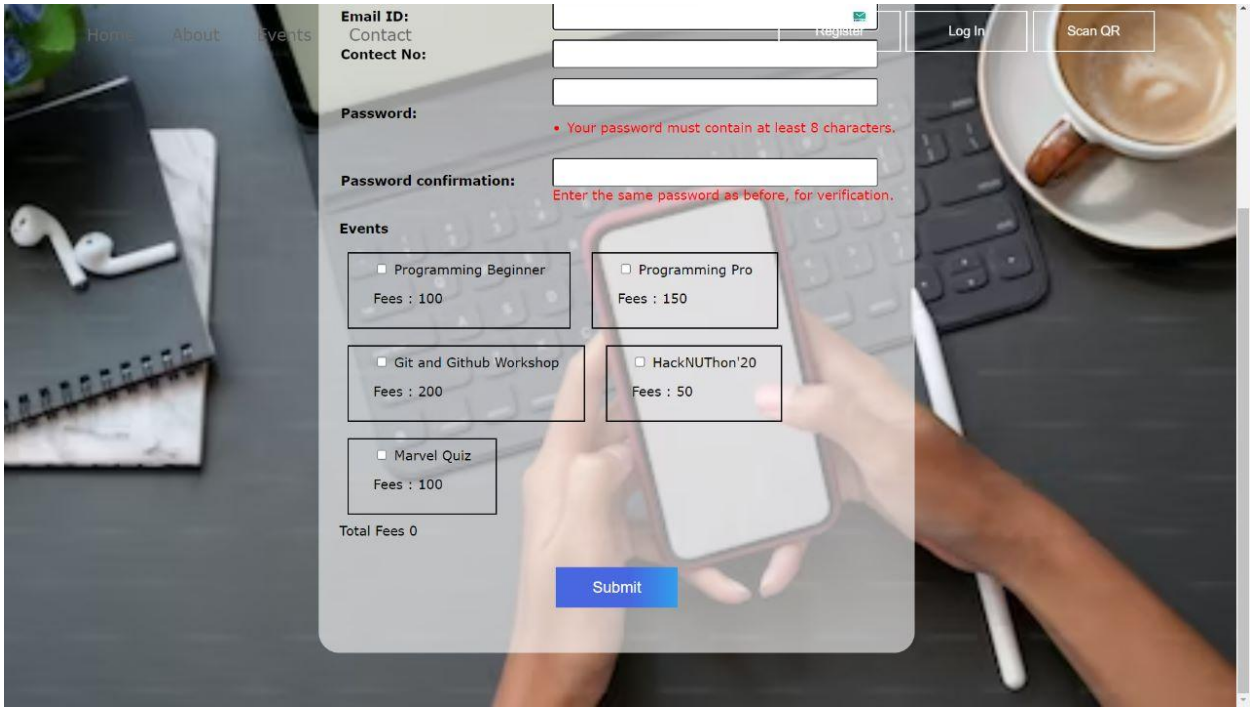
This is the home page to our web application:



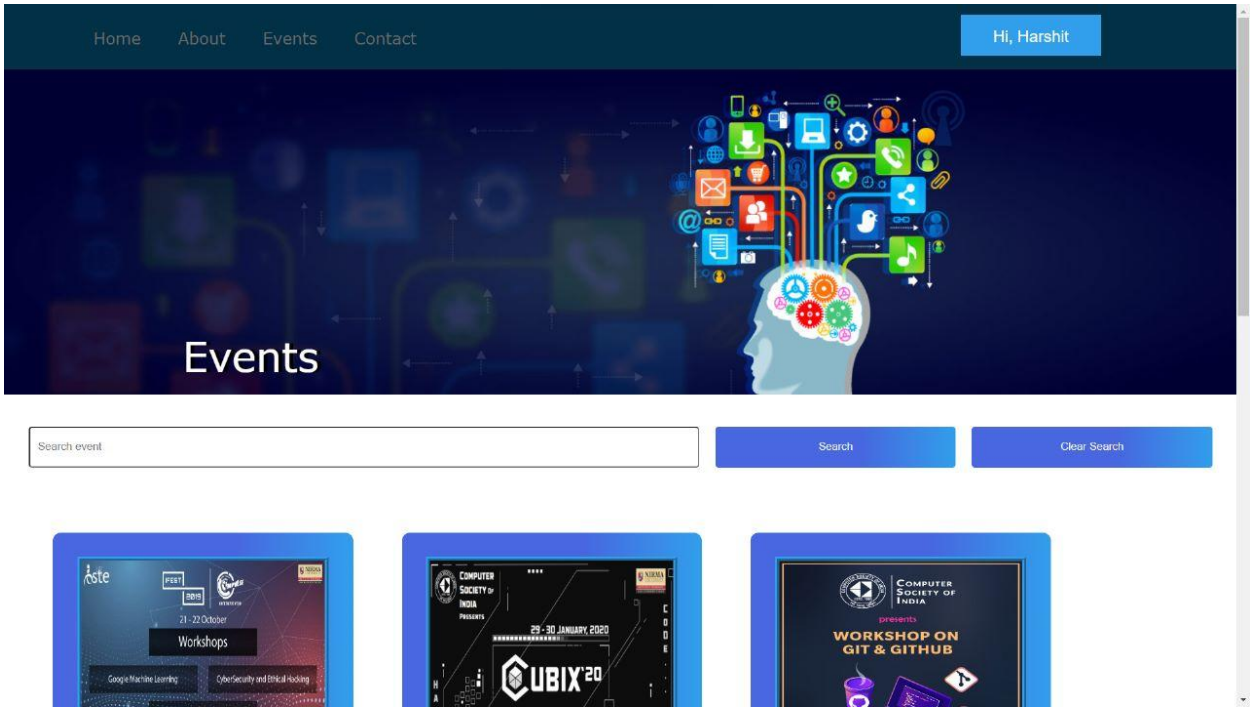
Here are the details about the organizer and their contact details.



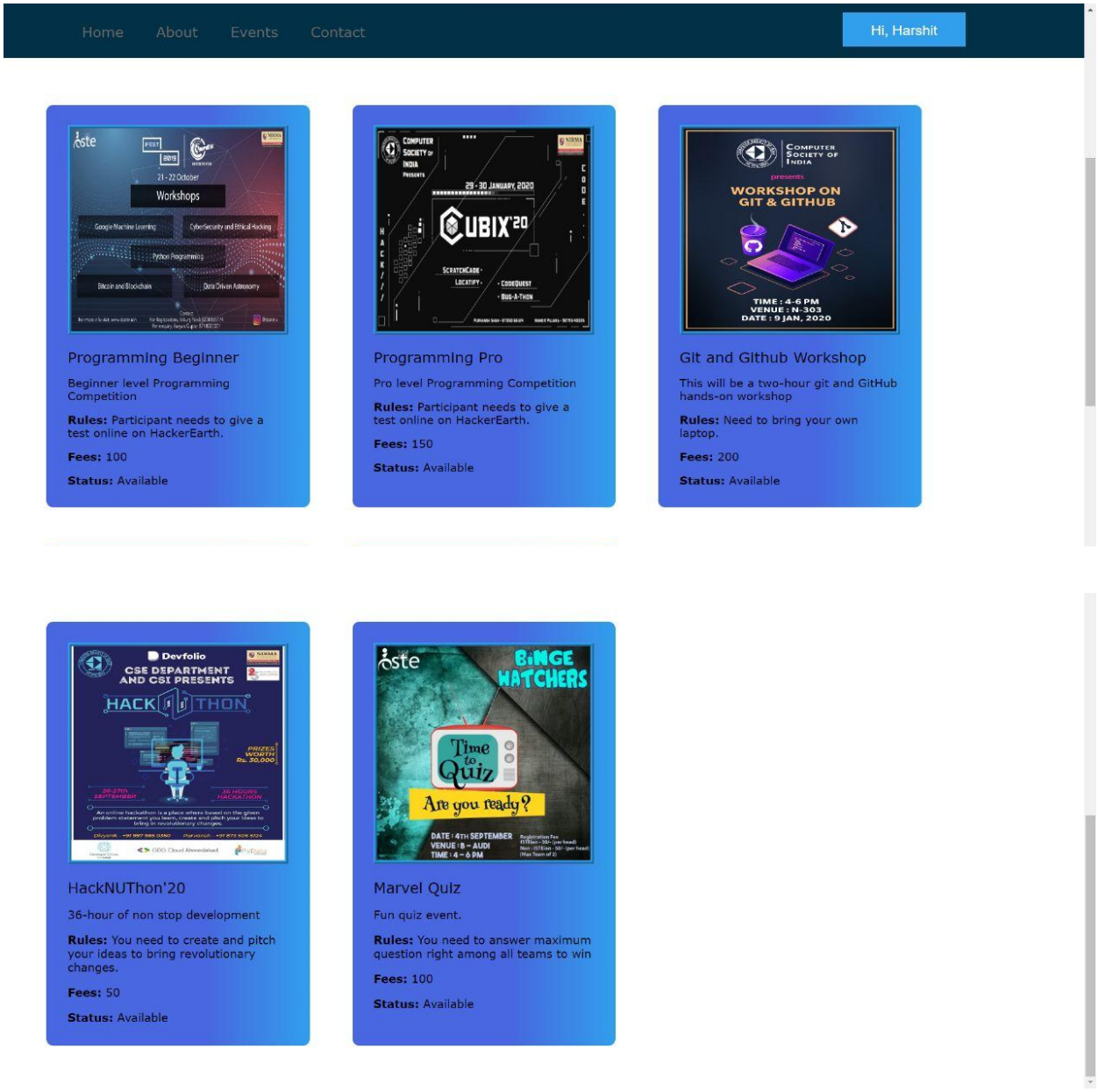
Registration Form & Payment for the Attendees :



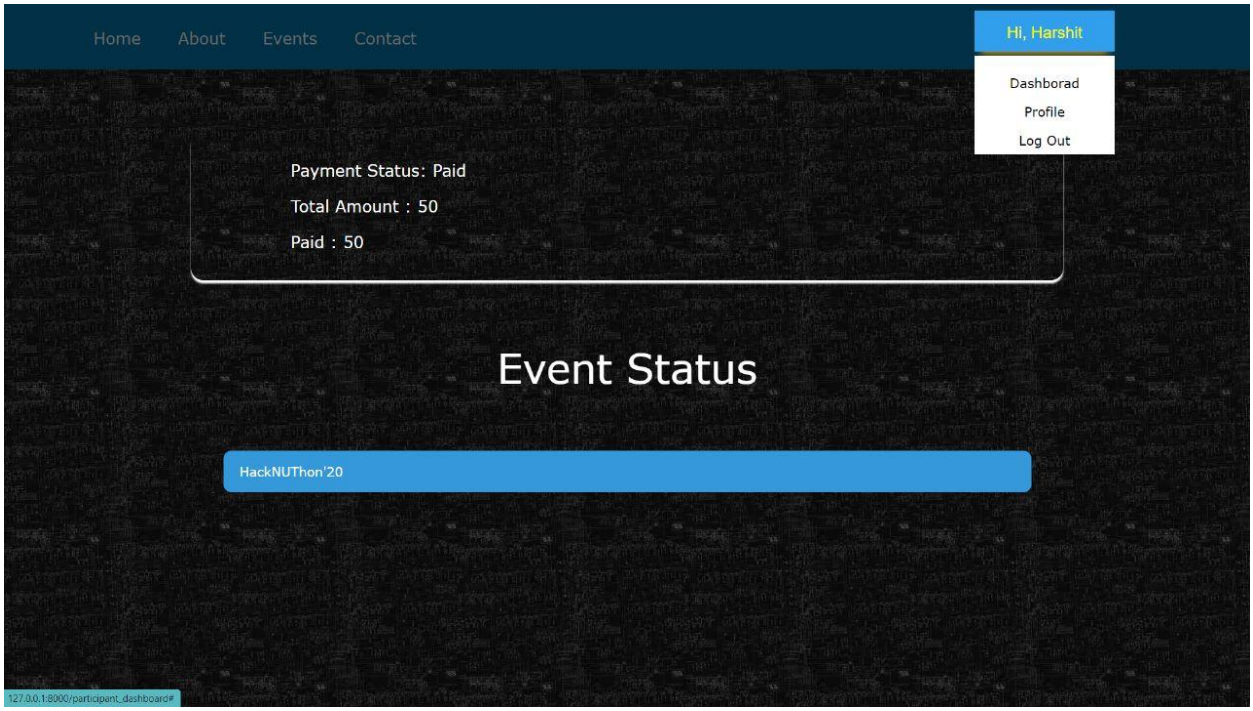
Events Section with search tool:



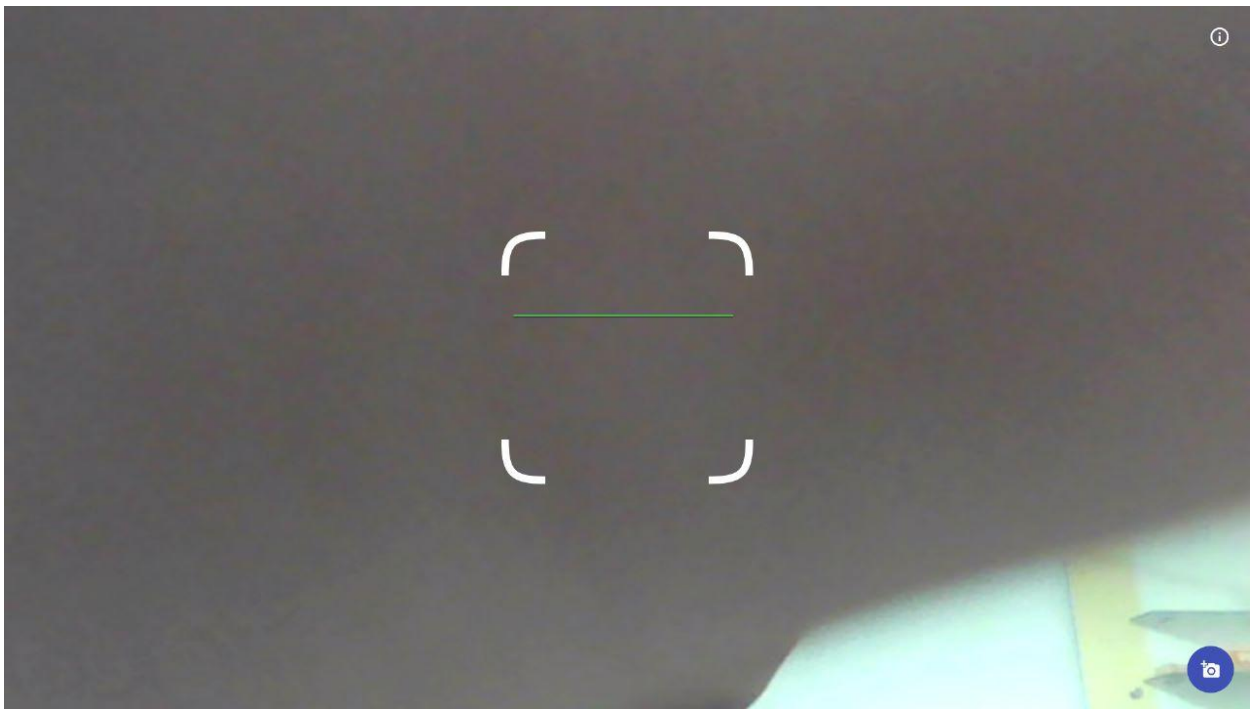
List of Events for booking :



Payment Successful Status & Registered Event Status:



QR Code Scanner :



9. SWOT Analysis

STRENGTH	WEAKNESS
• Reduce workload and stress • Reduce Complexity • Increase productivity	• Structured dataset required • Limited compatibility
OPPORTUNITY	**THREATS**
• Learn and implement the concepts of microservices and Security standards using cryptography • Learned the concepts of OOPS • Gained knowledge about MongoDB and its connectivity.	• Internet connectivity issues • Technology advancements • Regulatory Restrictions

10.PERT CHART

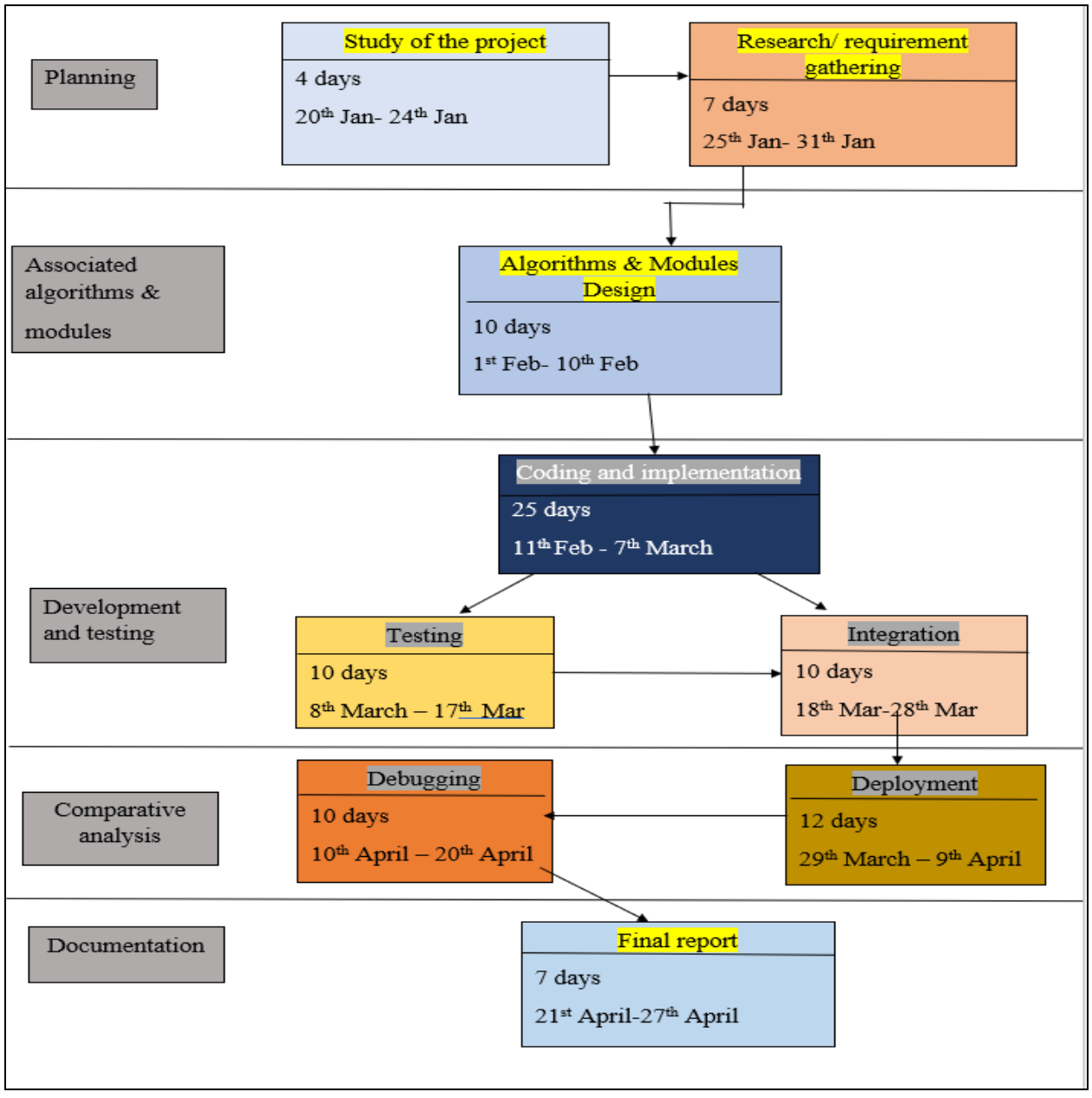


Fig 3: Pert Chart for the project

11. References

1. J. G. Lee and S. W. Kim, "A Lightweight QR Code-Based Authentication System for Mobile Devices," in Proceedings of the 2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom), 2015, pp. 505-510. doi: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP.2015.137
2. H. J. Kim, D. H. Kim, and K. H. Moon, "QR code-based secure access control system for IoT devices," in Proceedings of the 2017 IEEE 14th Intl Conf on Ubiquitous Intelligence and Computing and 2017 IEEE 14th Intl Conf on Autonomic and Trusted Computing and 2017 IEEE 17th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC/ATC/ScalCom), 2017, pp. 299-306. doi: 10.1109/UIC-ATC-ScalCom.2017.45
3. J. Kim and J. Lee, "A QR Code-based Mobile Authentication Framework for NFC Services," in Proceedings of the 2014 IEEE Intl Conference on Consumer Electronics (ICCE), 2014, pp. 128-129. doi: 10.1109/ICCE.2014.6775956
4. R. D. B. Dsilva and D. D. Dsilva, "Performance evaluation of MongoDB and MySQL for storage and retrieval of metadata," in Proceedings of the 2016 Intl Conference on Advances in Computing, Communications and Informatics (ICACCI), 2016, pp. 1377-1381. doi: 10.1109/ICACCI.2016.7732345
5. K. H. Moon, H. J. Kim, and D. H. Kim, "QR Code-Based Authentication for Secure Online Transactions," in Proceedings of the 2016 Intl Conference on Information and Communication Technology Convergence (ICTC), 2016, pp. 648-649. doi: 10.1109/ICTC.2016.7763488