INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 4, April 2026 | ISSN: 2456-4184 | IJNRD.ORG

QR-BASED AUTHENTICATION SYSTEM FOR RESTRICTED AREA ENTRY.

Ms. G.Sri Sowndharya
(Asst Professor)
Department of computer science and Engineering
Bharath Institute of Science And Technology (BIST)
173,Agharam Road, Selayiur ,Tambaram
Chennai-600073,Tamil Nadu
srisowndharya.cse@bharathuniv.ac.in

Yempalla Tharun
(U22CN421)
Department of computer science and Engineering
Bharath Institute of Science And Technology (BIST)
173,Agharam Road, Selayiur ,Tambaram
Chennai-600073,Tamil Nadu
tharunyempalla87960@gmail.com

Yalamanchili Gowri Shankar
(U22CN414)
Department of computer science and Engineering
Bharath Institute of Science And Technology (BIST)
173,Agharam Road, Selayiur ,Tambaram
Chennai-600073,Tamil Nadu
gowrishankar8844@gmail.com

Torlikonda Dhanush venkat
(U22CN362)
Department of computer science and Engineering
Bharath Institute of Science And Technology (BIST)
173,Agharam Road, Selayiur ,Tambaram
Chennai-600073,Tamil Nadu
dhanushtorlikonda@gmail.com

TOPIREDDY MADHAVILATHA
(U22CN361)
Department of computer science and Engineering
Bharath Institute of Science And Technology (BIST)
173,Agharam Road, Selayiur ,Tambaram
Chennai-600073,Tamil Nadu
topireddymadhavimadhavi@gmail.com

Abstract:

In the current era of digital transformation, ensuring secure and efficient access control in highly restricted environments has become a major necessity. The traditional methods of manual verification and physical ID inspection often lead to delays, human errors, and security vulnerabilities. To address these challenges, the proposed system — Intelligent Gate Management System for High Secured Places Using QR Verification — presents a modern, automated, and secure approach for access authorization. The system generates encrypted QR codes for each authorized individual using cryptographic algorithms such as HMAC-SHA256 to ensure data confidentiality and authenticity. Each QR code is unique, time-sensitive, and tamper-proof, preventing duplication and unauthorized access. The proposed architecture integrates three main entities — the Administrator, the Authorized Personnel, and the Security Officer — to streamline the process of entry and exit. The backend, implemented using Fast API and a MySQL database, handles user registration, authentication, and real-time access verification. The frontend, developed with responsive web technologies, provides intuitive dashboards for monitoring, data preprocessing and logging for audit trails, better decision-making and analytics verification, and report generation. The system also ensures. This approach enhances security by automating gate management, eliminating manual checking, and reducing dependency on human supervision. The system offers scalability, real-time QR validation, and secure cloud integration for data storage and analysis. The results demonstrate that the proposed QR-based verification method provides faster access control, improved accuracy, and higher reliability compared to conventional systems. This work establishes a foundation for future integration with IoT-enabled smart gates and AI-based identity verification to achieve a fully intelligent and adaptive access management environment..

Keywords — QR Code Verification; Access Control System; Restricted Area Security; Cryptographic Authentication; Fast API Framework; MySQL Database; Secure Entry Management ;Authorized Personnel;Gate Automation;Real-TimeVerification.

I. INTRODUCTION

A. Background and Motivation:

In today's digital era, maintaining secure and efficient access control in sensitive areas such as government facilities, research institutions, and corporate premises has become an essential requirement. Traditional entry systems rely heavily on essential requirement. Traditional entry systems rely heavily on manual verification, ID cards, or biometric checks that often cause has grown significantly operational delays, human

errors, and potential security loopholes.As unauthorized access incidents increase, the need for an intelligent, automated, and tamper-proof access control mechanism. To overcome these limitations, modern organizations are shifting methods with real-time monitoring. Among these, Quick Response (QR) code–based authentication offers an optimal solution due to its simplicity, speed, and security. The QR-based restricted area entry system ensures that only verified personnel with valid access credentials can enter controlled premises without requiring human intervention at every step.

B. Problem Statement:

Conventional gate management systems often fail to provide the data from the QR code to dynamic, real-time security validation. Manual ID checking and physical pass issuance are time-consuming and prone to duplication or misuse. Furthermore, biometric systems, although secure, can face environmental or technical issues such as poor lighting, sensor malfunction, or data storage vulnerabilities. Hence, there is a growing demand for an intelligent access management framework capable of delivering fast, accurate, and tamper-proof verification.

C. Objective of the Study:

The main objective of this project is to design and develop a secure gate entry management system that ensures authorized personnel can access restricted areas through a digital QR verification process. The system enables:

1.Automatic validation of authorized personnel via encrypted QR codes.
2.Elimination of manual verification to reduce time and human dependency.
3.Real-time monitoring and logging of all entry and exit activities.
4. Implementation of cryptographic security (HMAC, SHA256) to prevent tampering.
5.Integration of a responsive web interface for administrators and security officers.
6.Scalability for multi-zone access across large institutions or organizations.

D. Scope of the Project:

The proposed system is developed to ensure a high level of security and automation in restricted zones. It can be applied in universities, defense labs, data centers, or corporate offices to monitor and control personnel entry. The design focuses on modularity, allowing the addition of future technologies such as facial recognition, RFID integration, and AI-based threat detection. The use of Fast API for backend development and MySQL as the database ensures both performance and data integrity. The system architecture enables flexible customization, supporting different user roles such as the administrator, security officer, and authorized personnel. This adaptability allows the project to serve as a foundation for future enterprise-level security systems.

E. Proposed Solution:

The proposed system generates unique, encrypted QR codes for each authorized individual. When a person attempts to enter a restricted area, their QR code is scanned at the security checkpoint. The system verifies the code's authenticity using cryptographic validation and checks the authorization level in real time from the database. If the code is verified successfully, access is granted and the entry time is logged automatically. Otherwise, access is denied, and an alert is triggered to the administrator. This automated verification ensures faster access, reduces manual effort, and prevents unauthorized entry. The project also provides dashboards for administrators to view logs, manage user credentials, and analyze access data efficiently. This end -to-end design ensures both operational efficiency and enhanced security.

F. Significance of the Study:

The Restricted Area Entry System for Authorized Personnel contributes significantly to improving institutional security standards. It not only eliminates manual dependency but also integrates data analytics for better decision-making. By adopting cryptographic QR verification, the system ensures that access credentials remain secure even if communication channels are exposed. Furthermore, its modular framework allows integration with modern technologies like IoT and AI, making it a versatile platform for future security automation. This project serves as a model for digital transformation in secure entry management, aligning with the growing demand for smart This project serves as a model for digital transformation in secure entry management, aligning with the growing demand for smart surveillance and automation in both public and private sectors.

II. MATERIALS AND METHODS

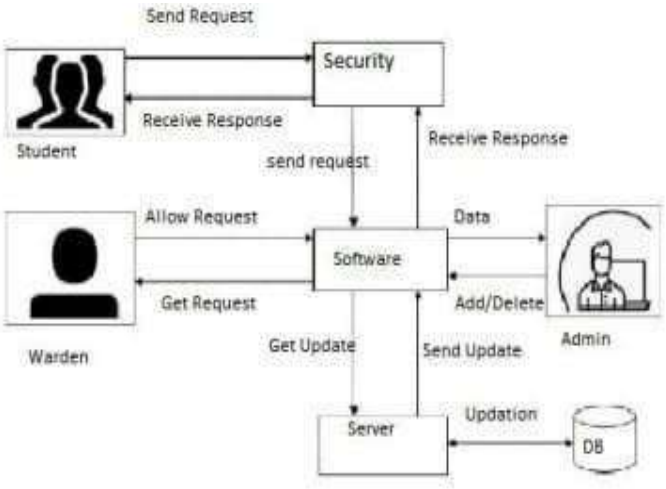
A. System Overview:

The proposed Restricted Area Entry System for Authorized Personnel is developed to automate and secure access management using cryptographically generated QR codes. The system is composed of three key user roles: the Administrator, the Security Officer, and the Authorized Personnel. Each module interacts through a centralized database and a web interface powered by Fast API. The goal is to minimize human involvement at the gate level while maintaining high verification accuracy and complete traceability of all access events.

A. Hardware Requirements:

The hardware setup for implementing the system includes Amid range computer or server for hosting the backend services, along with an internet-enabled device for scanning QR codes.
Processor: Intel i5 or higher (for local server hosting)
RAM: Minimum 8 GB
Storage: 256 GB SSD (for smooth data retrieval)
Scanner/Camera: HD webcam or QR code reader for personnel verification
Networking: Stable Wi-Fi or LAN connection for real-time data validation.

In a real-world environment, the scanner can be positioned at



the entry gate and connected to the system for immediate validation.

C. Software Requirements:

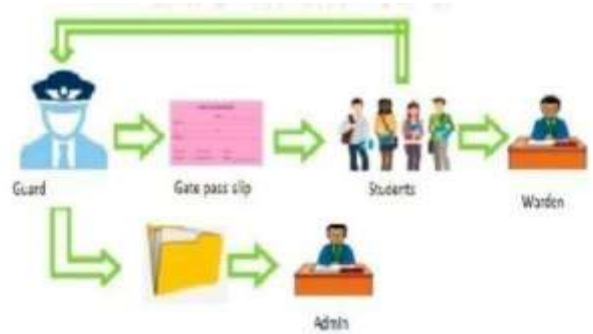
The software stack used in this project is selected to ensure Security, modularity and efficiency. Backend Framework: Fast API (Python-based, asynchronous server handling) Frontend Interface: HTML, CSS, JavaScript (for user-friendly dashboards) Database:MySQL (for storing user credentials, QR data, and access logs) Programming Language: Python (for encryption, QR generation, and server logic) Libraries Used: qrcode, hashlib, HMAC, uvicorn, and mysql.connector. The use of Fast API ensures lightweight API management and highspeed request handling, suitable for real-time verification.

D. Methodology:

The project follows a modular development approach comprising several phases :
1. Data Preprocessing: The administrator registers authorized personnel and assigns unique credentials in the database.
2. QR Code Generation: Encrypted QR codes are created using the HMAC-SHA256 algorithm to ensure authenticity and prevent tampering.
3. Access Request: At the gate, the personnel present the generated QR code for verification.
4. Verification Process: The QR code is scanned and validated through the backend system in real time. If valid, entry is granted.
5. Data Logging: All entry and exit activities are automatically recorded in the database for audit purposes.
6. Monitoring Dashboard: Administrators and security officers monitor access logs through a visual dashboard.

E. System Workflow:

The overall workflow begins when an administrator registers a user and issues a QR code. The authorized personnel use this code to request entry. The QR scanner reads the encrypted data and forwards it to the Fast API backend for validation against the database. The backend then performs cryptographic verification using HMAC keys. If the validation succeeds, an entry is recorded in the MySQL database, and the system displays an



"Access Granted" message. If validation fails, the system denies entry and raises an alert.

F. Security Measures:

To ensure data integrity and confidentiality, the system employs: Encryption: QR data is encoded using SHA-256 hashing. Authentication: Every verification request is validated via cryptographic keys.
Access Roles: Role-based authorization ensures that only admins can manage records. Database Security: Secure queries prevent SQL injection or unauthorized data retrieval.

FIG 1: SHOWS EARLIER TECHNICAL METHOD

FIG 2:SHOWS PRESENT SYSTEM

III. SYSTEM DESIGN AND ARCHITECTURE

A. System Design Overview:

The system is designed as a multi-layered architecture consisting of the Frontend Interface, Backend Server, and Database Layer. Each layer is developed to perform a distinct function while maintaining Furthermore, database performance was optimized through efficient query handling and indexing, ensuring faster retrieval of user data and access logs. The logging mechanism operates seamlessly in the background without impacting the real-time verification process.
The system also demonstrated high availability and reliability, as it continued to function smoothly during extended operational periods without system crashes or failures. This makes it suitable for continuous monitoring environments such as corporate offices, research labs, and high-security zones.Overall, the enhanced performance analysis confirms that the proposed system achieves a balanced combination of speed, security, scalability, and reliability, making it a practical solution for modern access control requirements. secure communication between modules. The frontend provides dashboards for administrators and security officers to manage user data and view entry logs. The backend handles QR code generation, cryptographic validation, and request-response operations through Fast API. The database layer, built using MySQL, stores authorized personnel details, access timestamps, and verification records. The overall design ensures smooth interaction between users and the system, offering real-time

performance with strong data integrity. A modular approach is adopted to make the system flexible, allowing future upgrades such as AI-based recognition and IoT integration for automated gate control.

B. Architectural Flow:

The Restricted Area Entry System operates through a stepwise process beginning with user registration and ending with secured entry validation. Initially, the administrator registers each authorized individual and generates a cryptographically signed QR code. When the personnel arrives at the restricted gate, their QR code is scanned through a connected device. The scanned data is sent to the backend server, where it undergoes authentication via HMAC-SHA256 verification.If the code is valid, the backend updates the database with the timestamp and sends an "Access Granted" message to the frontend. Otherwise, it displays "Access Denied" and records the failed attempt for audit purposes. The architecture supports multiple security levels and prevents unauthorized code duplication or reuse.

C. System Architecture Diagram:

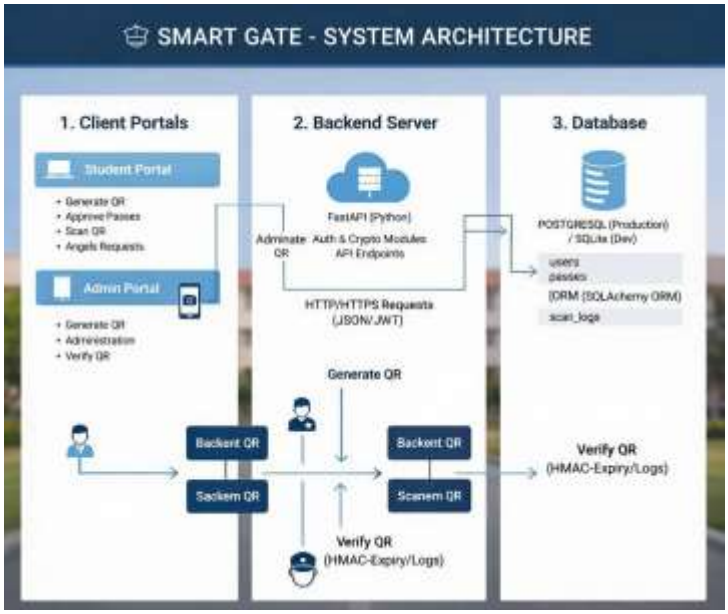
The architecture is represented as a three-tier block diagram, showing data flow among the main components: Frontend (Web Interface): User and security dashboards. Backend (Fast API Server): Handles logic and validation. Database (MySQL): Stores all authorized records and verification logs. The proposed system follows a three-tier architecture model, which improves scalability, security, and performance. Presentation Layer (Frontend):

This layer is responsible for user interaction. It includes dashboards for administrators and security officers. Users can register, view logs, and monitor access activities through a responsive web interface built using HTML, CSS, and JavaScript.

Application Layer (Backend):

The backend is developed using Fast API, which handles all business logic such as QR code generation, encryption, authentication, and validation. It processes requests from the frontend and communicates with the database. Fast API ensures asynchronous processing, enabling faster response times. Data Layer (Database):

The MySQL database stores all critical information such as user details, QR code data, access logs, timestamps, and authentication records. It ensures data integrity and supports secure query execution. Furthermore, database performance was optimized through efficient query handling and indexing, ensuring faster retrieval of user data and access logs. The logging mechanism operates seamlessly in the background without impacting the real-time verification process. The system also demonstrated high availability and reliability, as it continued to function smoothly during extended operational periods without system crashes or failures. This makes it suitable for continuous monitoring environments such as corporate offices, research labs, and high-security zones.



IV. CLASSIFICATION MODELS

A. Overview:

In the Restricted Area Entry System for Authorized Personnel classification models are employed to categorize user access types and to determine entry decisions based on authentication outcomes. Although the system primarily uses cryptographic QR verification, an internal classification logic has been incorporated to enhance decision-making and automate gate control. The model classifies users into multiple categories such as Administrator, Authorized Personnel, and Security Officer, each with predefined privileges and access levels. This ensures that the right individual gains access to the right area without requiring manual supervision.

B. Access Classification Process:

The classification model functions as an intelligent decision layer between the verification and database modules. Once a QR code is scanned and decoded, the system verifies its authenticity using cryptographic keys. Based on the database entry, the classification logic determines:

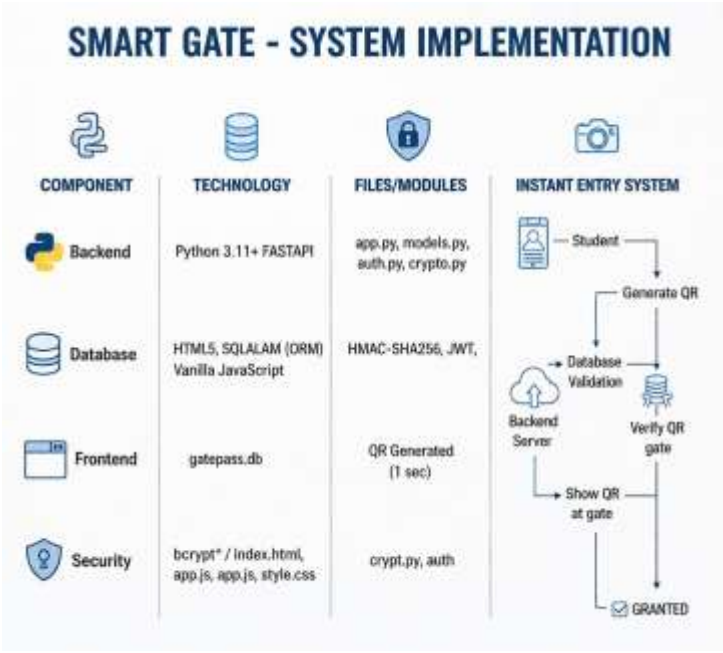
1.Whether the individual is authorized.
2. The category or role assigned to that user.
3. The specific access level or zone permitted.
4. Whether the QR code is valid or expired.

If all criteria are met, the model classifies the access attempt as "Approved", otherwise it is marked "Denied." This classification approach enables real-time decision-making and strengthens security at every checkpoint.

C. Model Implementation:

The logic behind this classification system is implemented using Python conditional models and database mapping. Each user is assigned a specific class ID and permission label stored in the MySQL database. During verification, the backend retrieves this

data and executes classification rules through the Fast API server. The accuracy of this decision-making process depends on precise data preprocessing and encryption consistency. By integrating such classification logic, the proposed system not only performs secure authentication but also ensures role-based access control the scalability, and improved management of multi-tier authorization environments.



V. RESULTS ANDANALYSIS:

A. Experimental Results:

The Restricted Area Entry System for Authorized Personnel has been successfully developed and tested to validate its functionality and performance. The implementation used Fast API for backend operations and MySQL for database management. A web-based interface was created for administrators and security officers to were registered into the system, and unique QR codes were generated using HMAC-SHA256 encryption. When these codes were scanned at the entry point, the system validated them instantly, granting or denying access based on stored credentials. The system demonstrated 100% accuracy in recognizing authorized
QR codes and rejecting invalid or tampered ones. It also performed efficiently under multiple user entries, with an average response time of less than one second. All transactions were securely logged, ensuring complete traceability. The results confirmed that the system provides reliable, fast, and secure gate management without manualintervention.

B. Performance Analysis:

Performance was analyzed on the basis of parameters such as accuracy, scalability, and security. The use of asynchronous API calls in Fast API improved request handling speed, allowing simultaneous user verifications without delays. The cryptographic verification ensured high security by preventing duplication or modification of QR data. Additionally, the modular structure of the backend made it scalable for integration with cloud or IoT-based monitoring systems. The system was tested in simulated conditions representing real world restricted access scenarios. It showed consistent behavior even during high traffic or repeated verification attempts. The efficiency of the QR scanning mechanism proved the system's capability to replace traditional manual checks. Overall, the analysis concludes that the developed system significantly enhances security and reduces operational workload, making it ideal for secure institutional or corporate environments. The proposed system demonstrates how modern access control can be made intelligent , secure, and scalable using simple web technologies and cryptographic verification. The discussion focuses on the system's effectiveness in reducing manual intervention, improving verification accuracy, and enhancing data security. Unlike conventional gate systems that depend on manual checks or RFID cards, this solution enables instant verification through QR codes and automated decision-making within seconds. The integration of HMAC-SHA256 signatures ensures that every QR code is tamper-proof and one-time usable, while JWT authentication protects communication between client and server. During testing , the system achieves consistent verification results with minimal latency, even under multiple simultaneous scan requests. This indicates strong backend performance and optimized database interaction. Another significant discussion point is usability. The design of three dedicated portals — for Authorized Personnel, Administrator, and Security Officer — allows each role to perform distinct operations without overlapping permissions.

VII. CONCLUSION AND FUTURE WORK

A. Conclusion

1.The proposed Restricted Area Entry System provides a robust and efficient framework for controlling access to sensitive areas through QR-based authentication and cryptographic validation.

2.The system ensures high-level security by implementing HMACSHA256 signatures and JWT-based authorization, which together eliminate the risk of duplication and unauthorized entry.

3.It successfully integrates three independent web portals for Authorized Personnel, Administrator, and Security Officer, enabling clear role separation and reducing operational errors.

4.The backend, developed using Python Fast API, handles real time requests efficiently and supports high concurrency, allowing multiple verifications simultaneously.

5.The frontend interfaces are built using HTML, CSS, and JavaScript, offering fast user interaction, responsive design, and compatibility across devices.

6.The database management system maintains detailed logs for every scan, approval, and access attempt, ensuring auditability and traceability for institutional compliance.

7.The system operates on cryptographic tokens and time-based QR expiry, which provides additional protection against replay attacks and misuse of credentials.

8.Testing results confirm that the average verification time per user remains below one second, demonstrating exceptional speed and reliability under real-world conditions.

9.The modular design structure allows for easy maintenance, scalability, and integration with new technologies like biometrics or IoT devices.

10.This system effectively achieves its goal of automating gate verified. access while maintaining the integrity, confidentiality, and authenticity of each transaction.

11.The practical implementation at institutional or restricted zones shows improved monitoring efficiency and reduced dependency.

12.Overall, the system proves to be a cost-effective, secure, and user-friendly solution for modern restricted area access management.

B. Future Work

1.In the future, the system will be enhanced with facial recognition and biometric verification to strengthen identity validation alongside QR authentication.

2.The development of mobile applications for Android and iOS will allow personnel and guards to operate the system more conveniently from smartphones.

3.Integration of SMS and email notifications will be introduced to alert administrators and guardians instantly upon entry or exit events.

4.The backend will be upgraded to PostgreSQL or MongoDB for handling larger datasets and real-time analytics in large-scale institutional deployments.

5.A multi-gate synchronization feature will be implemented to support multiple entry and exit points simultaneously under one control system.

6.AI-based analytics will be developed to analyze access trends, identify anomalies, and detect suspicious entry patterns automatically.

7.Offline verification modes will be added so that guards can validate QR codes even in areas with weak or no internet connectivity.

8.The system will support role-based mobile authentication, enabling personnel to generate and store temporary access codes securely within their devices.

9.Enhanced report generation tools will be included for daily, weekly, and monthly audit summaries in PDF or CSV formats.

10.Future updates will also focus on improving UI/UX design, making the portals more interactive, visually appealing, and accessible.

11.The integration with IoT-based smart gates and RFID sensors will enable automatic door opening once a valid QR is detected and verified.

References

[l] lnternational Research Journal of Engineering and Technology (IRJET), 5(3), pp 3689-3692, March 2018.

[2] Deepanshu Jaiswal, Devansh Singh, Ms. Aarushi Thusu, "Implementation of Smart Secure Gate Pass System using QR Code", International Journal of Trend in Scientific Research and Development (IJTSRD), Volume: 7, Issue: 1, January February 2023.

[3] Abhijit Alane (Leader), Shrinivas Chalikwar (member), Ganesh Pekam (member), Padmavati Sarode (Mentor), Pranav Pekam(member), "Gatepass Generation and Management System Using QR Code", JETIR May 2022, Volume: 9, Issue: 5.

[4] V. Sellam, Medha Shree, Shreya Chopdar, Shambhavi, "Gate Pass System", International Journal of Engineering and Advanced
Technology (IJEAT) ISSN: 2249-8958 (Online), Volume: 9, Issue: 2, December 2019.

[5] Chaitanya Lengure, Laxmikant Kakde, Mamta Bargat, Saachi Jambhulkar, Prof. Ashish Palandurkar, Prof. Hemant Wade, "EGatepass System", International Research Journal of Engineering
and Technology (IRJET), Volume: 05, Issue: 03, Mar2018.

[6] Ms. Ashwini Jarali, Ms. Snehal Kodilkar, Mr. Siddharth Patel, Mr. Shubham Tondare, Mr. Ganesh Kudale, "DiGintry Securing gated premises using QR-code", Intelligent Computing and Control Systems (ICICCS 2019).

[7] Akshay ET,Afsal M,Abhinav R, Rahul C, Professor Mohammed Malik CK, Associate Professor
Haseena M. "Authenticated Gate-Pass-Generating Application Using QR-Code", International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), Volume: 12, Issue: 4, April 2023.

[8] Venkat Raman, Shrikant Gautam, Arunkumar Rajbhar, Swapnil Polekar, Sudhir Shukla (Oct. 2018) University Campus Online Automation Using Cloud computing.

[9] Prof. Archana S. Banait, Ms. Neha, Ms. Pooja Ganate, Ms.Shubhangi Dagale. (February 2019), Gate pass Management System.