Secure Student Attendance System using QR Code and One Time Password OTP Authentication

Abhishek Kumar[1] Aditya Ranjan Bhaskar[2] Ms. Nidhi[3]
[1,2,3]Department of Computer Science Engineering
[1,2,3]Galgotias College of Engineering and Technology, Greater Noida, India

Abstract — The proposed system introduces a secure and efficient method for managing student attendance by integrating QR code scanning with One-Time Password (OTP) authentication. This version avoids repetition, strengthens the academic tone, and emphasizes both security and authenticity. During attendance, the student scans the QR code, which triggers an OTP sent to their registered mobile number or email. The student must then enter the OTP within a limited time frame to confirm their identity. This dual-layer authentication prevents proxy attendance, ensures data integrity, and enhances accountability. The system maintains encrypted records of attendance, offering real-time monitoring and easy integration with institutional databases. By combining QR technology with OTP verification, the solution provides a reliable, user-friendly, and tamper-resistant approach to student attendance management.

Keywords: E-Authentication; QR Code Technology; One-Time Password (OTP); Student Attendance Management; Secure Identity Verification; Two-Factor Authentication; Digital Attendance Tracking; Proxy Attendance Prevention; Time-Bound OTP Validation; Encrypted Data Storage; Mobile-Based Authentication; Academic Record Security; Real-Time Attendance Monitoring; User-Friendly Interface; Automated Verification System

JEL Codes: C88; D83; I23; O33; K24

I. Introduction

Attendance tracking is key in schools to gauge student engagement and maintain order. Modern QR code and OTP setups replace slow name-calling with secure, instant checks tied to personal phones. Traditional approaches to attendance tracking, such as manual roll calls or maintaining paper registers, are often inefficient and susceptible to inaccuracies. These methods not only consume significant time but also create opportunities for misuse, including practices like proxy attendance. With the increasing focus on digital transformation in the education sector, there is a clear demand for secure, reliable, and automated systems that can streamline attendance management while ensuring authenticity and accountability.

The proposed E-Authentication system integrates Quick Response (QR) code technology with One-Time Password (OTP) verification to establish a dual-layer authentication mechanism. A distinct QR code is generated for each student, serving as a secure digital identifier that is directly connected to their learning portfolio. During attendance, the student scans the QR code, which triggers the generation of a time-bound OTP sent to their registered mobile number or email. The student must then enter the OTP to confirm their identity, ensuring that attendance is marked only for the rightful individual.

This combination of QR code scanning and OTP validation enhances security by preventing proxy attendance and unauthorized access. It also provides real-time monitoring, encrypted data storage, and seamless integration with institutional databases. By leveraging widely accessible technologies such as smartphones and secure communication channels, the system offers a user-friendly and reliable solution for modern educational environments.

Ultimately, the E-Authentication system addresses the limitations of conventional attendance methods while promoting transparency, accountability, and efficiency. It represents a step forward in adopting secure digital practices within academic institutions, aligning with broader trends in educational technology and information security.

II. E-Authentication Literature Review

The evolution of attendance systems has moved from manual registers to digital platforms, driven by the need for accuracy, efficiency, and security. Early digital systems relied on biometric verification or RFID cards, which improved automation but introduced challenges such as high costs, maintenance issues, and vulnerability to misuse. These limitations encouraged researchers to explore lightweight, cost-effective solutions using mobile technologies.

QR code-based attendance systems emerged as a practical alternative because of their simplicity, low implementation cost, and compatibility with smartphones. Studies in this area highlight that QR codes can streamline attendance recording, reduce paperwork, and provide real-time data access. However, most QR-only systems face a critical drawback: the possibility of proxy attendance, where one student shares their QR code with another.

To strengthen security, researchers have proposed integrating multi-factor authentication methods. One-Time Passwords (OTPs) are widely recognized for their effectiveness in identity verification, as they are unique, time-bound, and difficult to replicate. Literature on OTP-based systems emphasizes their role in preventing unauthorized access and ensuring that authentication is tied directly to the rightful user. When combined with QR codes, OTPs create a dual-layer verification process that significantly reduces the risk of fraudulent attendance marking.

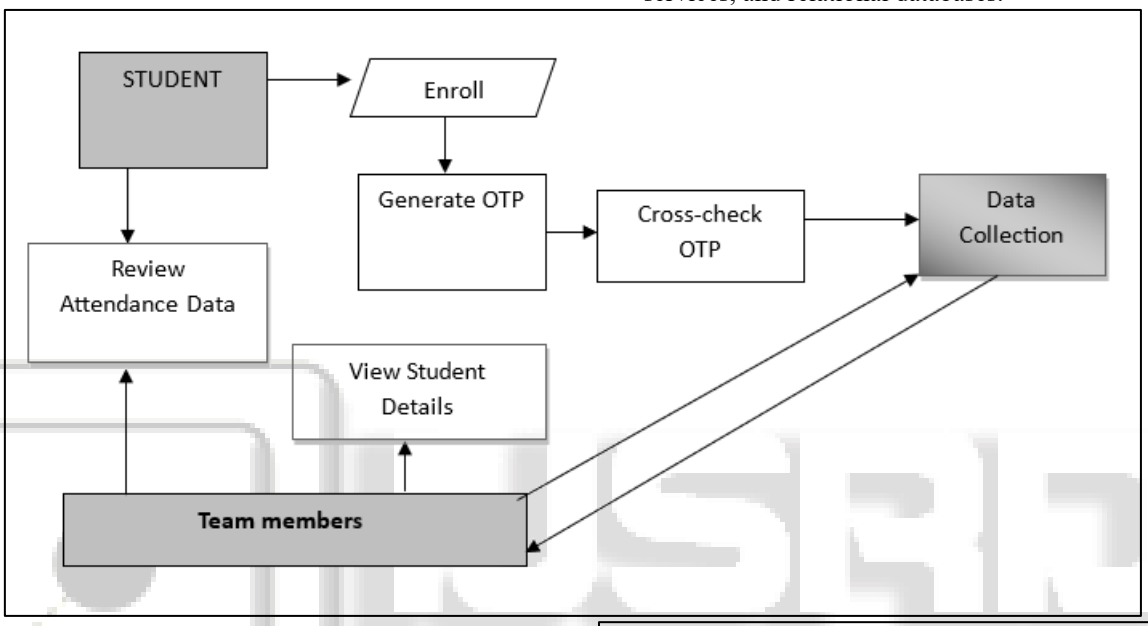
Despite these advances, existing studies often treat QR code or OTP mechanisms in isolation. Few systems have fully integrated both technologies into a unified framework for academic attendance. This gap highlights the need for a hybrid solution that leverages the convenience of QR scanning with the security of OTP validation. Such integration ensures not only efficiency but also authenticity, aligning with the broader goals of digital transformation in education.

III. Methodology

The methodology outlines the systematic approach adopted to design, develop, and evaluate the proposed E-Authentication system. The process is divided into several stages to ensure accuracy, security, and usability.

A. System Design

1) Requirement Analysis: Identify the limitations of existing attendance systems and define functional requirements such as QR code generation, OTP authentication, and secure data storage.
2) Architecture Planning: Develop a layered architecture consisting of a frontend interface (mobile/web application), backend server, and database.
3) Technology Selection: Choose appropriate tools and frameworks, such as QR code libraries, OTP generation services, and relational databases.



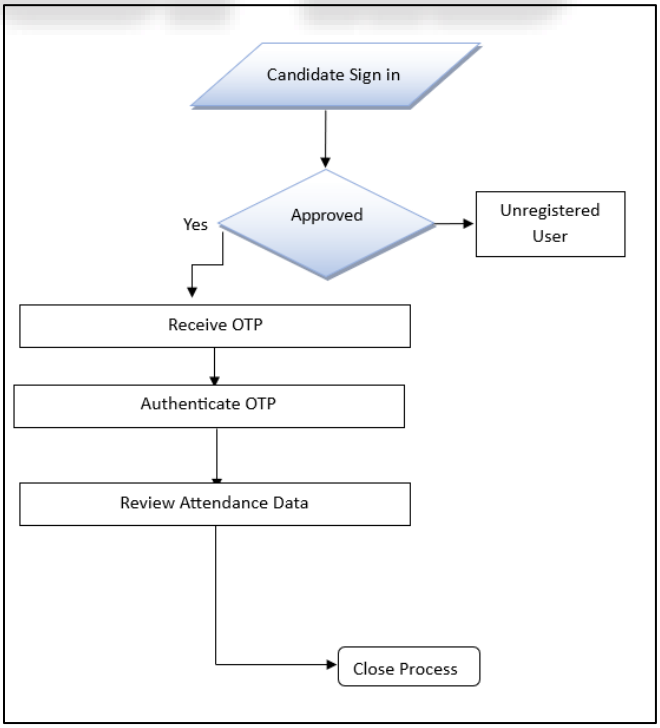
IV. Data Flow Diagrams (DFDs)

A Data Flow Diagram, often referred to as a *bubble chart*, is a widely used graphical tool for system modelling It provides a clear representation of how data enters a system, the processes that act upon it, and the resulting outputs.

DFDs are considered one of the most significant Modelling techniques in software engineering and information systems. They illustrate the major components of a system, including internal processes, the data utilized within those processes, external entities that interact with the system, and the pathways through which information flows.

By mapping the movement and transformation of information, DFDs help visualize how inputs are systematically converted into outputs. This graphical approach highlights both the logical flow of data and the transformations applied at each stage.

Importantly, DFDs can be constructed at varying levels of abstraction. At higher levels, they provide a broad overview of system functionality, while lower-level diagrams offer detailed insights into specific processes and data interactions. This hierarchical structuring makes DFDs a versatile tool for both conceptual design and detailed system analysis

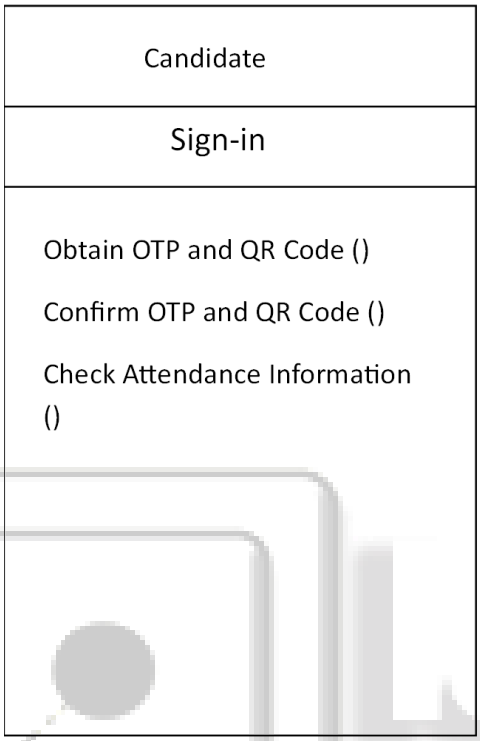


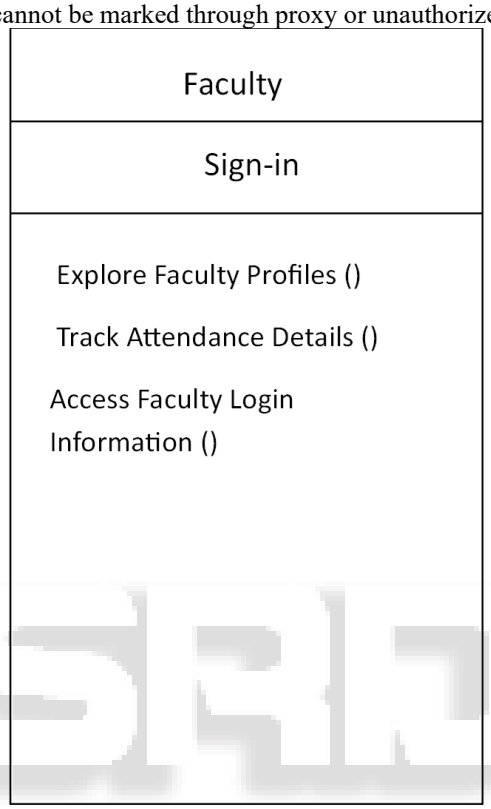
A. QR Code Integration

- Each participant is assigned an individualized QR code linked to their entry in the record system.
- QR codes are generated using secure algorithms to prevent duplication.
- Codes can be scanned via mobile devices or institutional scanners during attendance sessions.

B. OTP Authentication

- Once a QR code is scanned, the system generates a time-bound OTP.
- The OTP is sent to the student's registered mobile number or email.
- Students must enter the OTP within the validity period to confirm their identity.
- This dual-layer authentication ensures that attendance cannot be marked through proxy or unauthorized access.





C. Database Management

- A centralized database stores student profiles, QR code mappings, and attendance logs.
- Data is encrypted to maintain confidentiality and integrity.
- Attendance records are updated in real time and can be accessed by faculty or administrators.

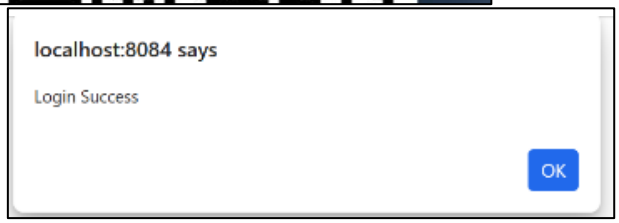
D. Implementation and Discussion

- Frontend: A mobile application or web portal for students and faculty.
- Backend: Server-side logic for QR validation, OTP generation, and attendance recording.
- Integration: Secure APIs connect the frontend with the backend and database.

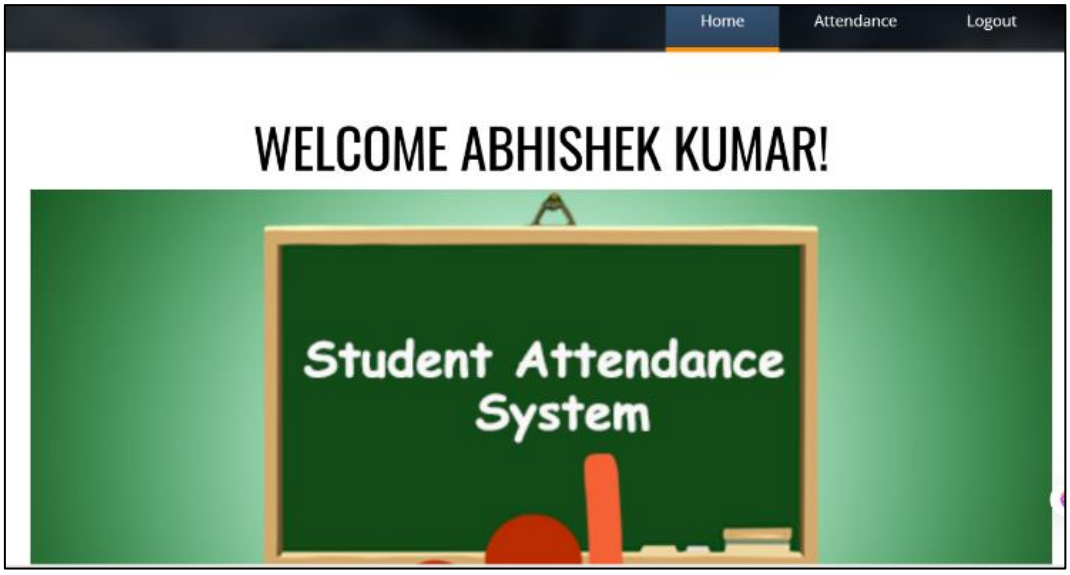
1) Login Page: serves as the entry point for both students and faculty into the E-Authentication system. It is designed to be simple, secure, and user-friendly, ensuring that only authorized individuals can access attendance features and records.

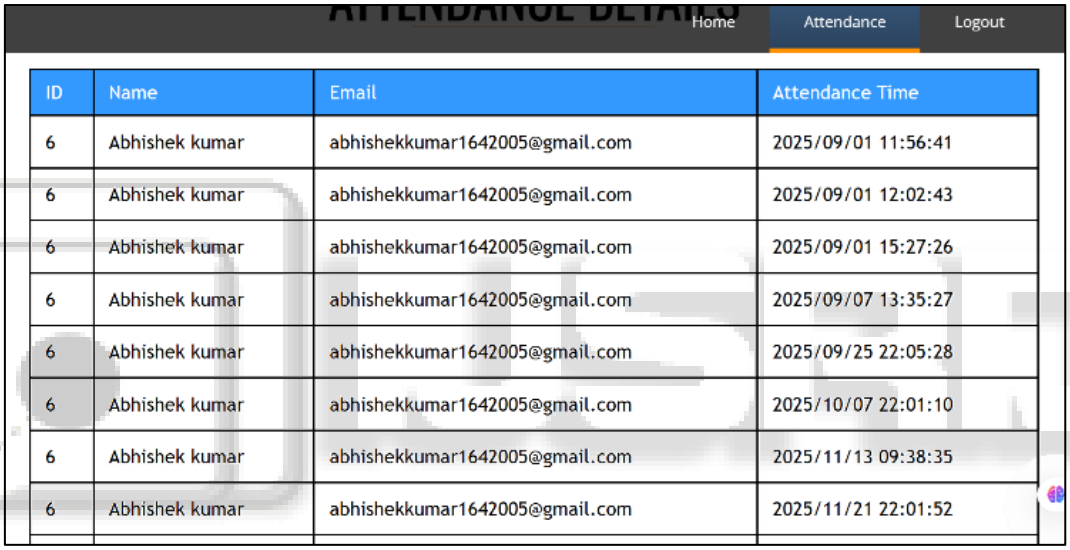
2) QR Code Verification for OTP: The integration of QR code verification with One-Time Password (OTP) authentication forms the core of the proposed E-Authentication system. This dual-layer process ensures that attendance is marked only by the rightful student, thereby eliminating the risk of proxy or fraudulent participation.

3) Login Success for OTP: The final stage of the E-Authentication process is the successful validation of the One-Time Password (OTP), which confirms the student's identity and grants access to the attendance system. This step ensures that attendance is marked only after dual verification, combining QR code scanning with OTP confirmation.



The attendance sheet in the proposed system is automatically generated once a student successfully completes the dual authentication process of QR code scanning and OTP validation. Unlike traditional paper-based registers, this digital sheet ensures accuracy, transparency, and security by recording attendance in real time.





ID	Name	Email	Attendance Time
6	Abhishek kumar	abhishekkumar1642005@gmail.com	2025/09/01 11:56:41
6	Abhishek kumar	abhishekkumar1642005@gmail.com	2025/09/01 12:02:43
6	Abhishek kumar	abhishekkumar1642005@gmail.com	2025/09/01 15:27:26
6	Abhishek kumar	abhishekkumar1642005@gmail.com	2025/09/07 13:35:27
6	Abhishek kumar	abhishekkumar1642005@gmail.com	2025/09/25 22:05:28
6	Abhishek kumar	abhishekkumar1642005@gmail.com	2025/10/07 22:01:10
6	Abhishek kumar	abhishekkumar1642005@gmail.com	2025/11/13 09:38:35
6	Abhishek kumar	abhishekkumar1642005@gmail.com	2025/11/21 22:01:52

E. Testing and Validation

- Functional Testing: Verify that QR scanning, OTP generation, and attendance marking work as intended.
- Security Testing: Ensure OTPs cannot be reused or intercepted.
- Usability Testing: Evaluate ease of use for students and faculty.
- Performance Testing: Assess system response time and scalability for large classrooms.

V. Implications and Limitations

A. Implications

Enhanced Security

1) Transparency and Accountability

- Every OTP attempt is logged, creating an audit trail that can be reviewed by faculty or administrators.
- This improves trust in attendance records and discourages fraudulent practices.

2) Transparency and Accountability

- Every OTP attempt is logged, creating an audit trail that can be reviewed by faculty or administrators.
- This improves trust in attendance records and discourages fraudulent practices.

3) Scalability

- The system can be deployed across classrooms and institutions without requiring expensive hardware.
- Since OTPs are delivered via mobile or email, the solution leverages existing communication infrastructure.

4) Integration with Academic Systems

- Attendance data captured through OTP verification can be directly linked to student information systems.
- This enables automated reporting, analytics, and performance tracking.

B. Limitations

1) Dependence on Network Connectivity

- OTP delivery requires stable internet or mobile network access.
- In areas with poor connectivity, students may face delays in receiving OTPs, affecting attendance marking.

2) Device Dependency

- Students must have access to a mobile phone or email-enabled device to receive OTPs.

– Those without such devices may be disadvantaged.

3) System Overhead

– Generating and validating OTPs for large groups simultaneously may increase server load.
– Institutions must ensure adequate infrastructure to handle peak usage.

4) Human Factors

– Students may enter OTPs incorrectly or fail to respond within the validity period.
– This can lead to failed authentication attempts and require manual intervention.

5) Privacy Concerns

– Storing and transmitting OTPs involves handling sensitive student data.
– Strong encryption and compliance with data protection standards are necessary to prevent misuse.

VI. CONCLUSION

The integration of QR code verification with One-Time Password (OTP) authentication provides a secure and efficient solution for managing student attendance in academic institutions. By combining these two mechanisms, the system ensures that attendance is marked only after dual verification, thereby eliminating proxy practices and enhancing the authenticity of records. QR codes offer convenience and speed in identity recognition, while OTPs add a dynamic, time-bound layer of security that strengthens trust in the process.

The proposed system not only improves accuracy and transparency but also aligns with the broader movement toward digital transformation in education. It reduces administrative workload, provides real-time monitoring, and creates tamper-resistant records that can be easily audited. Although challenges such as network dependency, device accessibility, and system scalability remain, these limitations can be addressed through infrastructure improvements and optimized system design.

In conclusion, the E-Authentication system demonstrates how accessible technologies like QR codes and OTPs can be leveraged to build a reliable, user-friendly, and secure attendance management framework. Its adoption has the potential to transform traditional attendance practices, ensuring accountability while fostering a modern, technology-driven academic environment.

REFERENCES

[1] Mohammad Mannan, P. C. Van Oorschot, “Security and Usability: The Gap in Real-World Online Banking”, NSPW‟07, North Conway, NH, USA, Sep. 18-21, 2007.
[2] antiphishinggroup, “Phishing Activity Trends Report”,from: http://www.antiphishing.org, Dec. 2008.
[3] Sang-Il Cho, hoonjae Lee, Hyo-Taek Lim, Sang-Gon Lee, “OTP Authentication Protocol Using Stream Cipher with Clock-Counter”, October, 2009.
[4] Jean-Daniel Aussel, “Smart Cards and Digital Identity”, Telektronikk 3/4. 2007. ISSN 0085-7130.
[5] Jose Rouillard, “Contextual QR Codes”, Proceedidngs of the Third International Multi-Conference on Computing in the Global Information Technology (ICCCGI2008), Athens, Greece, July 27-Augst 1, 2008.
[6] IETF RFC 4226, HOTP: An HMAC-Based One-Time Password Algorithm, Dec. 2005,
[7] ISO/IEC 16022:2000 – Information Technology – International Symbology Specification – Data Matrix, 2000.
[8] ISO/IEC 18004:2000 – Information Technology – Automatic Identification and Data Capture Techniques – BarCode Symbology – QR Code, 2000.
[9] Ohbuchi, E., Hanaizumi., H., Hock, L.A, “Barcode Readers using the Camera Device in Mobile Phones”, in Proc. of 2004 International Conference on Cyberworlds, pp.260-265, 2004.
[10] Reilly, D., Smolyn, G. and Chen, H., “Toward fluid, mobile and ubiquitous interaction with paper using recursive 2D barcodes”, Pervasive Mobile Interaction Devices 2007 (PerMID2007), workshop at Pervasive 2007, Toronto, Canada, 2007.

