BioQR Access Manager

Biometric + One-Time QR Code Access Control

Group Members :

1. Yogita Dhau Gore (2201623)
2. Anish Anil Kshirsagar (2201638)
3. Sakshi Nivrutti Raut (2201658)

Guide : Prof. A. S. Kunte

Introduction

- The BioQR Access Manager offers a smarter, more secure way to manage access control. It combines fingerprint authentication with one-time-use QR codes, making it extremely difficult for unauthorized users to gain entry.
- This dual-layer security approach not only strengthens protection but also keeps things simple for users—no passwords to remember, just a quick scan and you're in.
- The BioQR project is a secure file-sharing system that integrates biometric authentication with QR code-based file access. It leverages both mobile and web technologies to provide a seamless experience for users

Project Scope

Secure Access Management

Develop a comprehensive system utilising biometric verification coupled with one-time QR codes for maximum security assurance

Integration with cloud

Future updates will include integrating cloud storage like AWS S3 or Google Drive to enable secure, scalable, and remote file storage.

Dynamic QR Generation

Generate time-sensitive QR codes changing every 10-30 seconds to provide dynamic access credentials.

Audit Trails & Logging

Maintain complete logs of who accessed what, when and how long for accountability.

Project Objectives

01

Enable Easy User Access:

Provide a simple and seamless experience for users to authenticate and access files via both Android mobile app and web platform.

02

Implement Strong Security:

Develop a secure access system that combines biometric fingerprint authentication with dynamic, time-limited QR codes to prevent unauthorized access.

03

Ensure Secure File Management:

Allow users to upload, manage, and share files securely, with QR codes controlling access.

04

Support Cross-Platform Functionality:

Build a fully integrated solution that works smoothly across Android and web, with a shared backend and database.

05

Build a Scalable Architecture:

Design the system to accommodate future growth and enhancements, such as cloud integration, role-based access, and additional biometric methods.

Literature Survey

Biometric Authentication

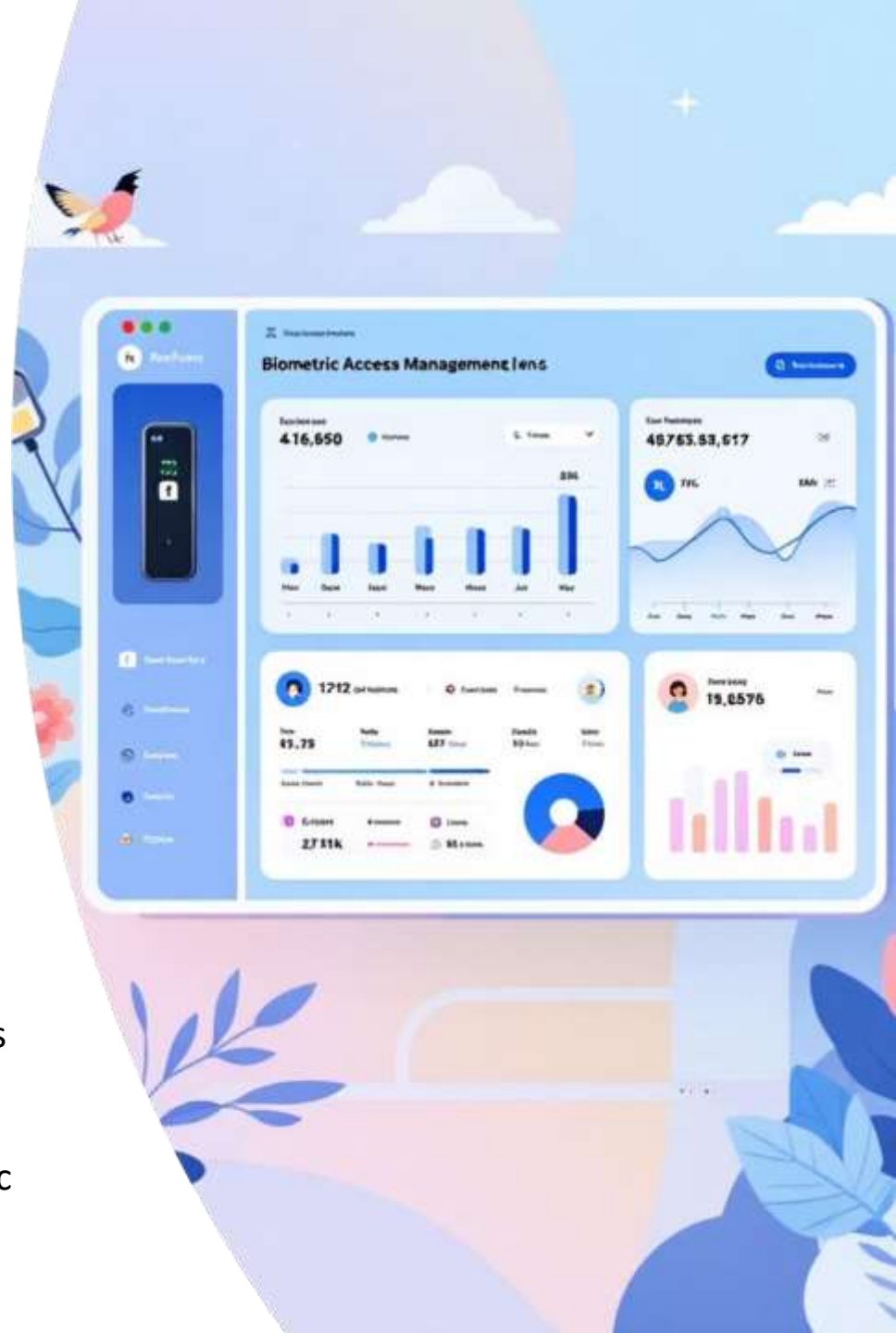
Fingerprint authentication, in particular, has been widely adopted due to its balance of uniqueness, convenience, and low cost. According to Jain et al. (2006), biometric systems provide strong identity assurance by linking access to unique physiological traits

QR Codes for Secure Sharing

QR codes have become an effective medium for sharing information quickly. Their application in secure systems, such as financial transactions and access control, has been widely researched. By combining time-limited tokens with QR codes, systems can ensure one-time, secure access. This aligns with prior research into ephemeral QR codes for secure data distribution.

Existing Gaps

While biometric authentication and QR codes are widely studied individually, there is relatively little research into their combined use for controlled file access. Current systems often focus on either device authentication or QR-based sharing without integrating both for stronger security. BioQR addresses this gap by merging biometric authentication with dynamic QR code generation.



Draft Problem Statement

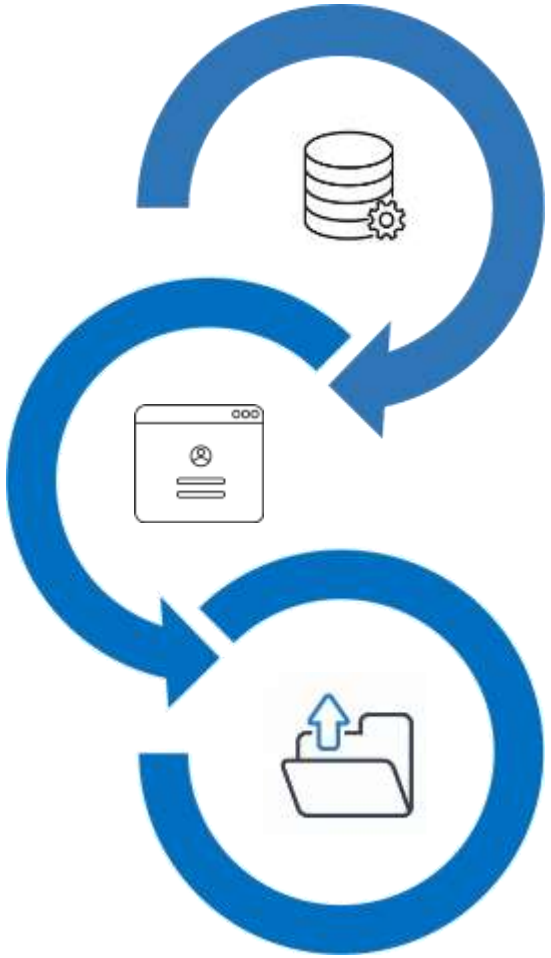
- Traditional ways like cards, passwords, and PINs can be easily stolen, lost, or copied.
- Physical access and digital access are usually handled separately, which causes:
  - Security isn't managed well
  - It's hard to keep a clear record of who accessed what
- There's no system that tracks access to both physical and digital places all in one place and in real-time.

Problem Statement:

"To develop a secure, cloud-based file access system using biometric fingerprint authentication and time-restricted, one-time QR codes to ensure that shared files are accessible only once and only by authorized users, preventing unauthorized access."

Work Completed Till Now

Requirements were finalized, the database schema was created, and the database was connected to both web and mobile platforms.



Web application was developed with login, dashboard, file upload, cloud storage integration, and file listing features.

We integrated the Android device’s biometric fingerprint authentication to securely verify the user’s identity before performing sensitive actions.

Work Pending

- Complete fingerprint verification and implement QR code expiry system.
- Develop QR scanning feature with proper token validation for secure file access.
- Build backend APIs and add encryption for files and biometric data security.
- Conduct End-to-End Integration Testing

  Web → Upload → Mobile Share → QR Scan → Access File

Thank You!