JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Innovative Secure File Access: Integrating QR Codes with Firebase

[1]P.Bhargavi, [2]S. Renu Roshini, [3]S. Sai Poojitha, [4]V. Sharmika Sanjana, [5]P. Radha Ramani, [6]Sk. Saniya
[1] Assistant Professor, Department of Computer Science and Engineering,
Narayana Engineering College, Nellore, Andhra Pradesh, India
[2-6] Students, Department of Computer Science and Engineering,
Narayana Engineering College, Nellore, Andhra Pradesh, India

Abstract : The Quick Response (QR) system gained popularity beyond the automotive industry because of its quick readability and larger storage capacity compared to standard UPC barcodes. Recently, college faculty members have been preparing and sharing notes with students, who then print them out for studying. However, this system is not user-friendly, eco-friendly, or efficient. To address these issues, I am developing an Android application to effectively share notes and materials with students. On the student side, they will use QR codes to quickly access notes and materials.

Key Words: Quick Response, UPC barcodes, QR Code, Android Application.

I. INTRODUCTION

In today's digital era, protecting and securely accessing sensitive information has become a top priority for individuals and organizations. As cyber threats become more sophisticated, the need for strong and user-friendly security measures has never been greater. One innovative solution is the use of QR codes for secure file access. This technology leverages the simplicity and prevalence of QR codes to provide a secure, efficient, and user-friendly means of accessing confidential files.

QR codes were first invented in 1994 by Denso Wave and have evolved from tracking automotive parts to becoming widely used in various industries. Their ability to store substantial amounts of data and ease of use has made them popular for tasks in marketing, payments, authentication, and secure communications.

The use of QR codes for secure file access capitalizes on these advantages, offering a seamless blend of security and convenience. Secure file access using QR codes is essential for enhancing security and streamlining user access in an increasingly digital world. QR codes offer a robust solution by embedding complex encryption keys and authentication tokens, which significantly reduces the risks associated with traditional password systems such as phishing, brute force attacks, and human error.

The purpose of a secure file-accessing application using QR codes is to provide a robust, user-friendly, and efficient method for safeguarding sensitive information. By integrating QR codes, the application enhances security through advanced encryption and multi-factor authentication, while simultaneously simplifying the access process for users. This approach minimizes the risks associated with traditional password-based systems, such as phishing and human error, and supports seamless, instantaneous file access.

II. EXISTING WORK

The first paper, "Enhancement of QR Code Capacity by Encrypted Lossless Compression Technology for Verification of Secure E-Document" by Ammar Mohammed Ali and Alaa Kadhim Farhan, presents a novel method to improve the data storage of QR codes through the application of encrypted lossless compression technology. Published in 2020, this paper addresses the need for secure transfer of various types of text information by enhancing the capacity and security of QR codes.

The second paper, "Secured Document Generation and Authentication Mechanism Using VSS and QR Code" by Deepen Saha, Shubham Sonar, Praful Telore, and Lalit Jadhav, provides a system for secure document generation and authentication using Visual Secret Sharing (VSS) and QR codes. Published in 2016, this paper emphasizes the secure creation and validation of documents by leveraging the strengths of VSS and QR code technologies.

The third paper, "Secure Data Sharing Using QR Code" by CH. Nava Mallika and T. Anil Karuna Kumar, which was published in 2021, focuses on the generation of QR codes containing confidential data for rapid and secure data sharing. This project highlights the efficiency andsecurity of using QR codes while maintaining the confidentiality of the shared data. "Development of QR Code-Based Data Sharing Web Application Using System Development Life Cycle Method" by Surya Tjahyadi discusses the creation of a web application in 2021 that allows users to manage QR codes. The application, called "Quick Save," is hosted on a website and provides services such as data storage, sharing, and QR code generation. These services are developed following the System Development Life Cycle (SDLC) method.

Limitations of Existing Systems

- In the Current System, it doesn't provide any security to the files.
- This system allows access only to students, who are eligible with their respective year.

Disadvantages

- It doesn't provide any security to the files.
- Unauthorized access, data breaches, and malware infiltration will occur.
- It is not a reliable system.

III. PROPOSED WORK

In this paper, I undertook the development of an Android application aimed at facilitating the seamless sharing of notes and educational materials with students.

The application design centered on leveraging QR codes for swift access to the aforementioned resources. To ensure efficient storage and retrieval of files, I integrated the Firebase system, which not only provides a robust storage solution but also enables global accessibility to the stored materials. Additionally, the system supports various file formats, including doc and pdf files, thereby catering to diverse academic needs.

By employing these features, the application aims to streamline the process of distributing educational content to students, ultimately enhancing their learning experience and academic engagement.

In this paper, there are two types of users: Faculty and Students. Faculty members can register and log in to the system. They can upload study materials and class notes onto the Firebase server. While uploading the files to the Firebase server, they can also generate a QR code using a QR Code Generation Algorithm. The QR code can then be shared with students for quick access to the materials and class notes. Students, on the other hand, can register and log in to the system. They can view their profile information, access documents uploaded to the server, and scan the QR code to access files from Firebase.

Advantages

- It offers Security.
- It accesses sensitive files, offering a seamless blend of security, accessibility, and ease of use.
- Quick Accessible.

Software Environment

Stakeholder Identification: Key stakeholders involved in secure file access, include faculty, and students.

Gather User Requirements: To gather user requirements that describe the desired features and functionalities of the application from their perspectives.

- Faculty: Register and log in, upload files, generate QR, view uploaded files, and delete files.
- Student: Register and log in, view profile, view uploaded files, and scan QR to access the required files.

IV. Development of Core Modules

Faculty Module:

In the Faculty Module, faculty members have the capability to register and securely log in to the system. Once logged in, they have the ability to upload various educational materials and class notes to the Firebase server. When uploading files to the server, faculty members can utilize a specially designed QR Code Generation Algorithm to generate a unique QR code. This QR code serves as a convenient way to share access to the uploaded materials and class notes with students, enabling quick and easy retrieval.

Student Module:

The Student Module provides students with the functionality to register and securely log in to the system. Once logged in, students can view their profile information and access documents that have been uploaded to the server by faculty members. Furthermore, students have the ability to view and scan the QR codes associated with the file access from Firebase, thereby facilitating efficient retrieval of educational materials.

QR Scan Module:

In the QR Scan Module, students are equipped with a QR scanner within our application, enabling them to read and verify the data encoded within QR codes. When the verification process is successful, the associated file will be opened, ensuring secure and controlled file access. If the verification process fails, the file will remain inaccessible, thereby ensuring the security of the system and its resources.

QR Generate Module:

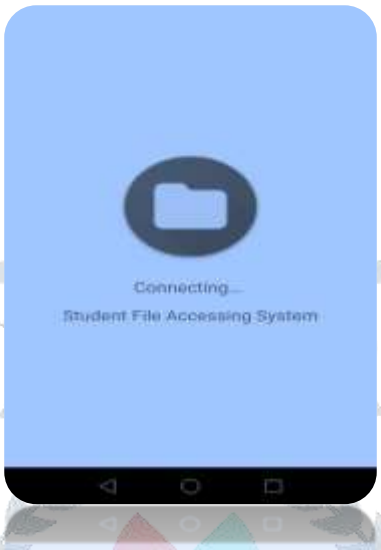
The QR Generate Module entails a detailed process which involves interpreting the bitstream as a sequence of bytes, dividing it into blocks, and computing and appending error correction bytes to each block. Through the interleaving of bytes from each block, a final sequence of 8-bit codewords to be drawn is produced. This process also includes the initialization of a blank square grid based on the version number, and the drawing of various function patterns onto the appropriate modules.

4.1. Development Environment

- **Programming Language:** JAVA, Android SDK
- **Database:** SQL (Structured Query Language) lite
- **Tool:** Android Studio 3. X
- **Front End:** Android UI

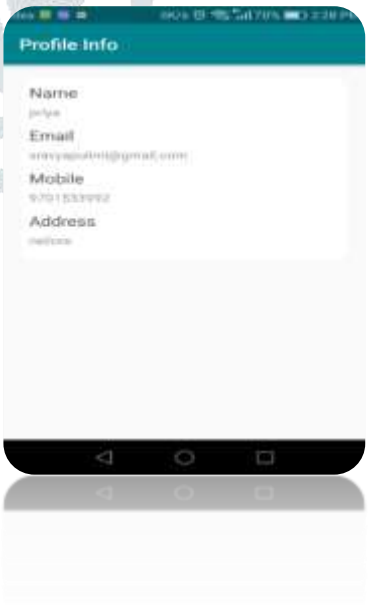
V.RESULTS AND DISCUSSION

5.1.Splash Screen



5.2.Login Page

5.3. Profile Info



5.4.Upload Files

5.5. View Documents

VI. CONCLUSION

This project involves the implementation of an Android application called "Firebase based File Accessing Using QR Code." The application securely stores files in the Firebase server and allows users to access the files from Firebase using a QR code. The system caters to two main types of users: faculty and students. Faculty members can share teaching materials and class notes with students through the application.

In conclusion, the use of QR codes for secure file access provides a user-friendly and robust solution for managing sensitive data.

Each file is associated with a unique QR code and multi-factor authentication ensures that only authorized users can access the files. The system also employs token verification and secure transmission to further enhance security. Detailed logging and monitoring functionalities help in detecting and preventing unauthorized access.

This system simplifies user experience while also strengthening data protection. It is an effective method for secure file sharing and access control in various applications. The robust token verification process and encrypted data transmission ensure the protection of files during access and transfer. Additionally, comprehensive logging and monitoring capabilities enable continuous oversight and swift detection of any suspicious activities, thus enhancing the overall integrity of the system. This method not only enhances user convenience but also adheres to high-security standards, making it a reliable solution for secure file management in diverse environments.

VII. REFERENCE

[1] Reardon, Marguerite (August 15, 2011). "Google just bought itself patent protection". CNET. CBS Interactive. Retrieved March 11, 2017.

[2] Perry, Douglas (July 16, 2011). "Google Android Now on 135 Million Devices". Tom's Guide. Purch Group. Retrieved March 11, 2017.

[3] Markoff, John (November 4, 2007). "I, Robot: The Man Behind the Google Phone". The New York Times. Retrieved February 15, 2012.

[4] Kirsner, Scott (September 2, 2007). "Introducing the Google Phone". The Boston Globe. Archived from the original on January 4, 2010. Retrieved February 15, 2012.

[5] Vogelstein, Fred (April 2011). "How the Android Ecosystem Threatens the iPhone". Wired. Retrieved June 2, 2012.