CHAPTER 2

LITERATURE SURVEY

In recent years, QR codes have been increasingly adopted for secure data sharing, authentication, and offline communication. Various researchers have proposed different methods, including encryption, steganography, and dual-layer QR codes, to improve the security and usability of file transfer systems. This section reviews significant works related to QR code–based secure file transfer systems and highlights the gaps that motivate the present study.

2.1 QR Code Generation in Web Systems

Sutheebanjard & Premchaiswadi (2010) developed a QR code generator using Drupal modules and the libqrencode C library on Ubuntu. They implemented QR creation through web forms using PHP hooks and command-line execution. This study demonstrated the possibility of dynamic QR code generation in web applications, but it did not focus on security or file confidentiality.

2.2 Dual-Layer QR for Confidential File Authentication

Patil & Parate (2017) proposed a two-level QR code method combining a public standard QR and a private textured pattern for storing confidential data. Using steganography, they embedded hidden private information into the QR code. This approach improved authentication and confidentiality but introduced high computational complexity, making it less efficient for lightweight file transfer.

2.3 Encrypted QR Chunks for File Transfer

Ramesh Babu et al. (2018) presented a secure file transfer mechanism where files were split into encrypted chunks, and each chunk was encoded into QR codes. This system ensured security during transmission and decoding but faced limitations in scalability since multiple QR codes were required for larger files, reducing user convenience.

2.4 Secure Transmission in IoT with Dynamic QR

Shen et al. (2020) introduced a secure information transmission scheme for IoT systems using SM4 encryption with dynamic QR codes. This prevented reuse of QR codes and improved security in IoT communication. However, the system was designed for IoT environments and not optimized for general-purpose offline file transfer.

2.5 Mobile-Based Secure File Sharing with QR

An IEEE study (2024) developed a mobile-based secure file sharing system using QR codes. The solution integrated encryption and authentication to protect files during transfer. Although it enhanced mobile usability, the system relied heavily on internet connectivity, limiting its use in offline scenarios.

2.6 AI-Enhanced Secure QR Codes

An IEEE work (2023) applied deep learning (CNN models) to improve QR code readability and tamper resistance. The study showed that AI techniques can make QR codes more robust in noisy or hostile conditions. While beneficial for secure decoding, this approach mainly focused on improving recognition rather than designing a complete file transfer system.

Criticism and Gap Identification

From the reviewed literature, it is clear that existing systems address specific challenges but fall short of providing a comprehensive solution. Web-based QR generators (Sutheebanjard & Premchaiswadi, 2010) enabled dynamic QR creation but ignored data security. Dual-layer QR approaches (Patil & Parate, 2017) enhanced confidentiality but were computationally heavy. Encrypted QR chunks (Ramesh Babu et al., 2018) offered strong protection but lacked scalability for larger files. IoT-based secure QR systems (Shen et al., 2020) ensured dynamic encryption but were domain-specific. Mobile QR file-sharing solutions (IEEE, 2024) improved usability but required internet support. AI-based QR security (IEEE, 2023) enhanced detection but did not address usability for file transfer.

Therefore, the identified **research gap** is the lack of a **secure, offline, cross-platform, and user-friendly QR code–based file transfer system**. The proposed project bridges this gap by developing a solution that integrates **encryption, QR-based**

access, and local network hosting, ensuring fast, private, and reliable file transfer without internet dependency.