Secure File Sharing System Using Qr Code and Aes Encryption

Babisha Princess P[1], Dharshini S[2], Jerofiya C S[3], D Kaavya[4]
[1,2,3,4]*Department of Information Technology, Arunachala College of Engineering for Women*
doi.org/10.64643/IJIRTV12I8-190081-459

***Abstract*— With the rapid growth of digital technologies, file sharing has become an essential part of communication in educational institutions, corporate organizations, and personal applications. However, the increasing dependence on online platforms has also raised serious concerns regarding data security and privacy. Many existing file-sharing systems rely on traditional authentication methods such as passwords or publicly shared links, which are often weak and vulnerable to unauthorized access, data interception, and misuse. As a result, sensitive information can be easily exposed, leading to data breaches and loss of confidentiality.**

To address these challenges, this project presents a secure file sharing system that integrates Advanced Encryption Standard (AES) encryption with QR code technology. In the proposed system, files are first encrypted using AES, ensuring that the data remains unreadable to unauthorized users even if the file is intercepted during transmission or accessed without permission. To further enhance security, the encryption key or secure access information required for decryption is embedded within a QR code. This QR code is shared only with authorized recipients, allowing controlled and secure access to the encrypted file.

The use of QR codes simplifies the process of secure key distribution while reducing the risk of key exposure. Authorized users can scan the QR code using a standard device to retrieve the required information and decrypt the file safely. This combination of strong encryption and QR-based access control provides an additional layer of protection without increasing system complexity. The proposed system offers improved confidentiality, prevents unauthorized access, and ensures secure data transmission. It is suitable for applications where data privacy and security are critical, such as academic document sharing, business communication, and cloud-based storage systems.

***Index Terms*— Secure File Sharing, AES Encryption, QR Code Technology, Data Security,Cryptography, Access Control, Information Privacy, Secure Key Distribution, Encrypted Data Transmission, Authentication, Confidential Data, Cyber Security, Digital File Protection, Data Confidentiality.**

I. INTRODUCTION

In the digital age, the rapid growth of information technology has led to an exponential increase in the exchange of digital data across networks. File sharing has become an essential requirement in various sectors such as corporate organizations, educational institutions, healthcare systems, and government services. Despite the convenience and efficiency offered by modern file-sharing platforms, security remains a major concern.Unauthorized access, data leakage, interception, and tampering of sensitive information pose serious threats to individuals and organizations alike.

Traditional file-sharing methods often rely on simple authentication mechanisms such as passwords or publicly accessible download links. These methods are highly vulnerable to brute-force attacks, phishing, link sharing, and man-in-the-middle attacks. In many cases, once a file-sharing link is compromised, the confidentiality of the shared data is lost entirely. Therefore, there is a critical need for secure file-sharing solutions that ensure confidentiality, integrity, and controlled access to data.

Cryptography plays a vital role in safeguarding digital information. Among the various encryption algorithms available, the Advanced Encryption Standard (AES) is widely recognized as one of the most secure and efficient symmetric encryption techniques. AES offers strong protection against cryptographic attacks while

maintaining high performance, making it suitable for encrypting large files. Due to its reliability and efficiency, AES has been adopted as a standard encryption algorithm in many security applications.

In addition to encryption, secure key distribution is a major challenge in file-sharing systems. Sharing encryption keys through insecure channels can expose sensitive data to unauthorized users. Quick Response (QR) codes provide an innovative solution to this problem. QR codes are capable of storing encrypted data, keys, or secure access references and can be easily scanned using standard devices. Their fast readability, high storage capacity, and ease of use make them suitable for secure data exchange.

This paper proposes a secure file sharing system that integrates AES encryption with QR code technology to enhance data security and access control. In the proposed system, files are encrypted using AES before transmission or storage, ensuring that the data remains protected even if intercepted. The encryption key or secure access reference is embedded within a QR code and shared only with authorized users. Only users with access to the correct QR code can decrypt and retrieve the original file.

By combining strong encryption with QR-based secure key distribution, the proposed system addresses the limitations of traditional file-sharing methods. The system provides enhanced confidentiality, prevents unauthorized access, and ensures secure and efficient data transmission. This approach is particularly suitable for applications requiring high levels of data security, such as corporate communication, cloud storage, and sensitive document sharing.

II. LITERATURE REVIEW

Secure file sharing has been an active area of research due to the increasing demand for safe and reliable data transmission. Many researchers have focused on using cryptographic techniques to protect digital information from unauthorized access. Encryption-based approaches are widely accepted as an effective solution for maintaining data confidentiality during storage and transmission.

Several studies highlight the effectiveness of the Advanced EncryptionStandard (AES) for securing digital data. AES is a symmetric encryption algorithm known for its high security, fast processing speed, and resistance to cryptographic attacks. Researchers have shown that AES performs efficiently even when encrypting large files, making it suitable for real-time and cloud-based file-sharing systems. Compared to older algorithms such as DES and Triple DES, AES offers stronger security and better performance.

In recent years, QR code technology has gained attention in the field of information security. QR codes have been used in applications such as secure authentication, mobile payments, and access control systems. Some researchers have proposed QR-based authentication methods where encrypted credentials or access information are embedded within QR codes. These studies demonstrate that QR codes provide a convenient and fast way to share sensitive information while reducing the risk of manual key entry errors.

A few existing file-sharing systems use QR codes to share download links or access credentials. However, many of these systems do not apply strong encryption to the actual file content, which limits their security. On the other hand, some encryption-based file-sharing solutions focus only on data encryption and ignore secure key distribution, which can expose the encryption key to attackers if shared through insecure channels.

From the reviewed literature, it is clear that there is a gap between strong encryption techniques and secure, user-friendly key distribution methods. Very few systems combine AES encryption with QR code-based secure access in an integrated manner. This gap highlights the need for a secure file sharing system that uses AES for data protection and QR codes for safe and controlled key distribution. The proposed system aims to address these limitations by providing a balanced solution that ensures strong security while maintaining ease of use.

III. METHODOLOGY

The methodology of the secure file sharing system focuses on ensuring the confidentiality, integrity, and controlled access of files. The system is designed

using a combination of AES encryption and QR code technology, with a step-by-step approach to secure file sharing.

File Upload
The process begins with the user selecting a file to be shared. The system supports multiple file types, including documents, images, and PDFs. This ensures flexibility for different user requirements.

AES Encryption
Once a file is selected, the system generates a unique AES secret key for that file. The file is then encrypted using the AES algorithm, converting the data into an unreadable format. This ensures that even if the file is intercepted or accessed by unauthorized users, the content remains protected.

QR Code Generation
After encryption, the AES key or a secure access reference is embedded into a QR code. This QR code acts as a secure token and is shared only with authorized recipients. Using QR codes reduces the risk of key exposure and eliminates the need for manually sharing sensitive information.

Secure File Sharing
The encrypted file and its QR code are sent to the intended recipients. The system ensures that the QR code is transmitted securely, allowing only authorized users to access it.

File Decryption
The recipient scans the QR code using a QR scanner to retrieve the AES key or access information. Using this key, the encrypted file is decrypted, restoring it to its original format. This process ensures that only users with the correct QR code can access the file.

Access Control and Storage
All files are stored in encrypted form, providing security even if the storage system is compromised. The system maintains controlled access by verifying the QR code during decryption, preventing unauthorized users from accessing sensitive data.
This step-by-step methodology ensures that files are shared securely, encryption keys are safely distributed, and only authorized users can accessthe information. The combination of AES encryption and QR code-based access provides a balance of strong security and user-friendly operation.

III. ARCHITECTURE

The secure file sharing system follows a simple and modular architecture designed to ensure data security and ease of use. The system consists of key components that work together to encrypt files and control access using QR codes.

The User Interface Module allows users to upload files, generate QR codes, scan QR codes, and download files. It acts as the main interaction point between the user and the system.

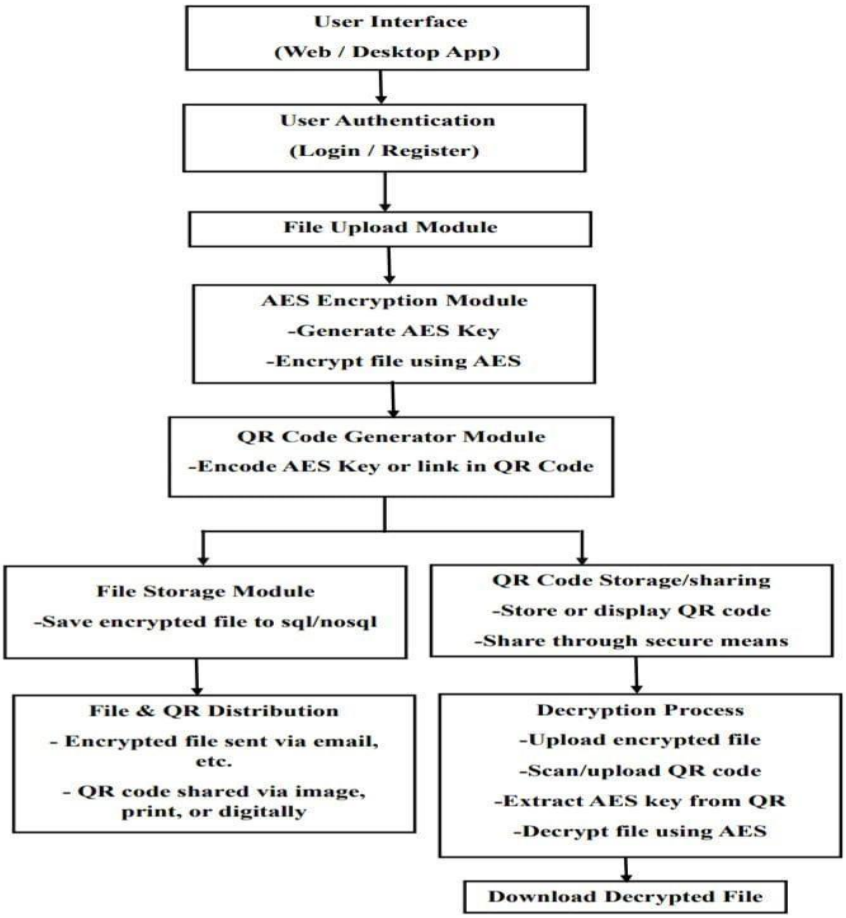
The Encryption Module encrypts the uploaded files using the Advanced Encryption Standard (AES). This ensures that the data remains protected during storage and transmission.

The QR Code Module generates a QR code that contains the encryption key or secure access information. This QR code is shared only with authorized users and helps avoid direct key sharing.

The Authentication Module verifies the QR code during the scanning process and ensures that only valid users can access the encrypted file.

The Storage Module stores files in encrypted form, providing security even if the storage system is accessed without permission.

Overall, the system architecture combines AES encryption and QR codebased access control to provide a secure, reliable, and user-friendly file sharing solution.



IV. IMPLEMENTATION

The secure file sharing system using QR code and AES encryption is implemented in a structured and modular manner to ensure security, reliability, and ease of use. The implementation focuses on encrypting files securely, generating QR codes for controlled access, and allowing authorized users to decrypt files without exposing sensitive information.

The implementation begins with the file upload process, where the user selects a file to be shared. The system supports different file formats such as documents, images, and PDFs. Once the file is uploaded, a unique AES secret key is generated for that file. This key plays a crucial role in ensuring data confidentiality.

In the encryption phase, the uploaded file is encrypted using the Advanced Encryption Standard (AES). AES is chosen due to its strong security and fast performance. The encryption process converts the original file into an unreadable encrypted format, ensuring that the data remains protected even if it is accessed by unauthorized users. The encrypted file is then stored securely in the system or transmitted through a secure channel.

After encryption, the QR code generation module comes into operation. The AES key or a secure reference to the encrypted file is encoded into a QR code. This QR code acts as a secure access token and is shared only with authorized recipients. Using a QR code for key distribution reduces the risk of key exposure and eliminates the need for manual key sharing.

On the receiver side, the authorized user scans the QR code using a QR code scanner. The system extracts the encrypted key or access information from the QR code and verifies the user's authenticity. Once verified, the AES key is used to decrypt the encrypted file and restore it to its original format. This process ensures that only users with the correct QR code can access the file.

Overall, the implementation successfully integrates AES encryption with QR code-based access control. The system ensures secure file storage, safe key distribution, and controlled file access while maintaining a simple and userfriendly workflow. This makes the system practical for real-world secure file sharing applications.

V. RESULTS & DISCUSSION

The proposed secure file sharing system was tested with different types of files, including documents, images, and PDFs, to evaluate its performance, security, and usability. The results showed that all files were successfully encrypted and decrypted without any data loss, confirming the effectiveness of the AES encryption module. The encryption process added minimal delay, demonstrating that the system can handle files efficiently without affecting user experience.

The QR code module also performed well, generating unique QR codes for each file securely. Authorized users were able to scan the QR code and retrieve the encryption key smoothly. This confirmed that QR codes can be

effectively used for secure key distribution, reducing the risk of unauthorized access or key exposure.

Overall, the system ensures data confidentiality, integrity, and controlled access. Even if an encrypted file is intercepted or the storage is accessed by unauthorized users, the data remains unreadable without the correct QR code. Users found the system simple and convenient, as the QR-based access eliminates the need for manually sharing encryption keys.

The discussion shows that combining AES encryption with QR code technology provides a strong and practical solution for secure file sharing. The system is suitable for real-world applications, such as corporate communication, cloud storage, and educational document sharing, where security and ease of use are both important.

VI. CONCLUSION

The secure file sharing system using AES encryption and QR code technology provides a reliable and user-friendly way to protect sensitive data. By encrypting files before sharing and using QR codes to distribute the decryption key securely, the system ensures that only authorized users can access the information. This approach effectively safeguards data confidentiality, integrity, and access control while keeping the process simple for users. The testing results show that files of various types can be securely shared and decrypted without errors, demonstrating the system's efficiency and reliability. Overall, the proposed solution offers a practical and strong method for secure file sharing in educational, corporate, and personal applications.

REFERENCES

[1] J. Daemen and V. Rijmen, The Design of Rijndael: AES – The Advanced Encryption Standard, Springer, 2002.
[2] W. Stallings, Cryptography and Network Security, 7th ed., Pearson, 2017.
[3] ISO/IEC 18004, "Information technology – QR Code specification," 2015.
[4] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
[5] B. Schneier, Applied Cryptography, 2nd ed., John Wiley & Sons, 2015.
[6] NIST, "Advanced Encryption Standard (AES)," FIPS PUB 197, 2001.
[7] S. Singh and N. Sharma, "Secure Data Transmission Using AES and QR Code," International Journal of Computer Applications, vol. 176, no. 12, pp. 1–6, 2020.
[8] K. Kumar, R. Gupta, and P. Verma, "QR Code Based Secure Data Sharing," International Journal of Engineering Research & Technology, vol. 9, no. 4, pp. 210–215, 2021.
[9] M. Patel and H. Shah, "A Review on AES Algorithm for Secure Data Transmission," International Journal of Innovative Research in Computer and Communication Engineering, vol. 7, no. 5, pp. 45–50, 2019.
[10] R. Sharma and S. K. Singh, "Secure File Sharing Using Encryption and QR Codes," Journal of Information Security and Applications, vol. 54, pp.102–110, 2020