A Review: Safer Document Exchange Protecting Documents using OTP, Authentication, and QR Codes

1st Harsh Somani
Computer dept. GHR COEM
Pune, India
harsh.somani.cs@ghrcem.raisoni.net

2nd Harshvardhan Shekhawat
Computer dept.
GHR COEM
Pune, India
harshvardhan.shekhawat.cs@ghrcem.raisoni.net

3rd Himanshu Zanzad
Computer dept.
GHR COEM
Pune, India
himanshu.zanzad.cs@ghrcem.raisoni.net

4th Narsing Kadam
Computer dept.
GHR COEM
Pune, India
narsing.kadam@raisoni.net

***Abstract*—Sensitive document communication must be done securely in the digital age. Conventional approaches frequently fail to provide enough protection against tampering and unwanted access. By combining One-Time Passwords (OTPs) with authentication methods and Quick Response (QR) codes, this article suggests an improved document protection solution. By using OTPs as a dynamic authentication factor, the suggested solution makes sure that every access request is verified with a distinct, time-sensitive code. The technique enables quick and easy authentication when combined with QR codes, which act as a secure connection between the user and the document. An OTP is generated when users use a mobile device to scan the QR code. Only those who are authorized can see or download the content because access to the document is allowed upon entering the OTP. This two-pronged strategy greatly reduces the chances of data breaches, phishing scams, and illegal access. Additionally, user experience is given top priority in the system's design, which strikes a compromise between strong security features and usability. While OTPs offer an extra degree of protection, QR code integration streamlines the authentication procedure. This study shows how well OTPs and QR code- based authentication work together to improve document security through thorough analysis and application. The suggested system provides a scalable solution that may be applied to a variety of industries where document secrecy is essential, such as gov- ernment, healthcare, and finance. Organisations can strengthen their digital document exchange procedures against new security threats by implementing this integrated approach.**

***Index Terms*—Data protection, information integrity, digital verification, OTP authentication.**

I. Introduction

Strong cybersecurity measures are now more important than ever in the modern digital environment, where private data is continuously transferred between networks. Cyberattacks like ransomware, phishing, identity theft, and data breaches are becoming more common and pose serious risks to businesses in a variety of industries, including vital infrastructure, government, healthcare, and finance. Static passwords and simple access controls are examples of traditional security methods that are no longer adequate to combat modern attackers. Therefore, it is essential to use sophisticated and multi-layered authentication methods to guarantee data availability, secrecy, and integrity. This study offers a dependable and expandable method for safeguarding digital documents by combining One-Time Password (OTP) authentication with QR code technology in a secure document exchange framework. The suggested so lution lowers the danger of unwanted access by using OTPs as a dynamic authentication technique to generate time-sensitive codes that are only valid for a set amount of time [1]. By encapsulating authentication information and enabling smooth communication between users and document repositories, QR codes provide a safe and intuitive user experience. The solution offers dual-layered protection by integrating these two technologies, reducing the vulnerabilities related to single-factor authentication techniques. By limiting access to critical documents to authorised users, the method reduces the possibility of interception or misuse. Additionally, usability is given top priority in the system's design, enabling users with different levels of technical proficiency to safely access information without sacrificing operational effectiveness. Protecting data while it's in transit and at rest is crucial for cybersecurity frameworks [2]. By combining OTP with QR code-based authentication, a proactive defence against unwanted access is offered, boosting confidence and regulatory compliance. Because of the framework's industry adaptability and ability to be incorporated into pre-existing security infrastructures, businesses can get a flexible and affordable solution. Through this study, we hope to show how carefully applied advanced authentication mechanisms may greatly improve document security and provide a safer online environment. The suggested framework provides a creative, effective, and safe method of managing documents, assisting businesses in protecting important data while tackling new cybersecurity issues.

II. LITERATURE SURVEY

A. Existing System

Digital signatures, email verification, and static passwords are the mainstays of current secure document exchange systems. These techniques, however, are susceptible to online dangers including phishing, identity theft, and illegal access. Stronger authentication is provided by more recent methods that use QR codes and One-Time Passwords (OTPs) to get around these problems. By guaranteeing that only authorised users may access important data, encrypted QR codes further improve security and streamline procedures in industries like banking, healthcare, and education.

B. Proposed System

By combining One-Time Password (OTP) authentication with QR code technology, the suggested solution protects document exchange and guarantees that sensitive data is only accessible by authorised users. A special QR code is created when a document is shared, and in order to view it, the recipient needs to scan it and provide a time-sensitive OTP. This technique offers a straightforward yet extremely safe means of document sharing across networks. Important attributes: • Dual-layered Security: Prevents data breaches and unwanted access by combining OTP and QR codes. • User-friendly Interface: This interface is simple to use and permits smooth document sharing without sacrificing security. • Scalable Solution: Ideal for a range of sectors where data security is essential, including finance, healthcare, and education.

C. Features of the System

A number of cutting-edge features are included in the suggested document exchange system to improve user experience and security. By integrating OTP verification with QR code scanning, it integrates Two-Factor Authentication (2FA), guaranteeing that only authorised users can access confidential documents. Users may safely save and manage their files with the ”My Documents” feature, and they can share papers with a wider audience or with particular people thanks to the versatile sharing choices provided by ”Private Shares” and ”Public Shares.” Users can quickly track and access documents shared with them by using the ”Received” section. The system also has a ”Reduce Size” option for document compression, which speeds up sharing and conserves storage space. An easy-to-use interface for managing files, viewing activities, and controlling permissions is offered by a centralised ”Dash- board.” By enabling users to swiftly access documents by scanning codes without requiring complex steps, the ”Scan QR” feature streamlines authentication. When combined, these characteristics offer a safe, effective, and intuitive document interchange environment that is appropriate for sectors where data security and accessibility are critical.

D. Need for the System

Secure document exchange has grown to be a top priority for both individuals and organisations in today’s digital environment. Conventional techniques like email sharing and passwords are frequently susceptible to online dangers including phishing, hacking, and illegal access. A more secure and effective solution is crucial as data privacy laws become more stringent and sensitive data requires more robust security. By incorporating cutting-edge authentication techniques like OTP and QR codes, the suggested system overcomes these difficulties and guarantees that only authorised users can access documents. Additionally, it streamlines document management, uses file compression to save storage space, and offers a smooth experience without sacrificing security. In industries like finance, healthcare, and education, where maintaining the privacy of sensitive information is essential to compliance and trust, this approach is particularly necessary. All things considered, it provides a dependable, expandable, and easy-to-use platform to safeguard documents from new online dangers.

TABLE I
LITERATURE SURVEY

Title	Results
Remote File Sharing System for Education Institution	secure document sharing [2]
Laboratory Access Implementing QR Code	Improved accuracy [3]
QR Code Document Authentication and Retrieval	Secure QR-OTP [4]
Enhancing Digital Security: A QR Code and OTP-Based E-Authentication System [5]	Strong 2FA system
Securing E-Medical Documents Using QR Code	Paperless, encrypted sharing [6]
Secured Authentication of Online Documents Using Visual Secret Sharing on QR Code [7]	High security
E-Medical Application using QR Code with OTP Generation [8]	2-Level QR
An Introduction to Using QR Codes in Web Portals for Synchronizing Calendar Events Over Phones [9]	Avg. decoding speed

III. MOTIVATION

Secure document exchange is now more important than ever due to the rise in cyberthreats and data breaches. Sensitive information can no longer be adequately protected from misuse and unauthorised access using conventional techniques like email exchange and passwords. This prompted the creation of a system that combines QR code authentication with One-Time Passwords (OTP) to guarantee that only authorised users can access documents. The objective is to offer a very safe, effective, and easy-to-use platform that enhances usability and confidence while satisfying the increasing needs for data protection in industries like banking, healthcare, and education.

IV. OBJECTIVES

- Make QR codes that lead to secure, time-limited URLs: Because QR codes are created with time-limited links, there is less chance of abuse and documents can only be accessed for a predetermined amount of time.
- Send an OTP to the recipient’s phone number or email address for 2FA: Before allowing access, a one-time password (OTP) is given to the recipient’s registered phone number or email address, adding an extra degree of security and confirming their identity.
- Send an OTP to the recipient’s phone number or email address for 2FA: Before allowing access, a one-time password (OTP) is given to the recipient’s registered phone number or email address, adding an extra degree of security and confirming their identity.
- Allow access only through a valid OTP and QR code: To guarantee that only authorised users may access or read the shared content, document access is rigorously restricted to users who supply both a valid OTP and a QR code.
- Monitor access to documents and ensure traceability: Every document access event is logged by the system, which records information like the user’s identity and the time of access. This enables administrators to keep an eye on usage and ensure responsibility.

V. METHODOLOGY

The system flow diagram shows the organised workflow of the suggested system for Secure Document Exchange Using OTP, Authentication, and QR Codes. Each of the methodology’s several modules guarantee digital document protection, accessibility, and controlled sharing.

A. Verification of the user

The first step in the procedure is for users to register or log in to the system. The dashboard is only accessible by authenticated users. This guarantees that verified entities are responsible for document uploading and distribution.

B. The Dashboard Interface

The user is shown a dashboard with four main tabs after successfully logging in:

- This is a list of the user-uploaded documents.
- Files provided with unfettered access are known as public shares.
- Files shared with restricted access that need authentication are known as private shares.
- Files shared with the logged-in user by others are referred to as received files.
- Additionally, users can upload, compress, and download file versions that are optimised for size using the dashboard’s Reduce Section.

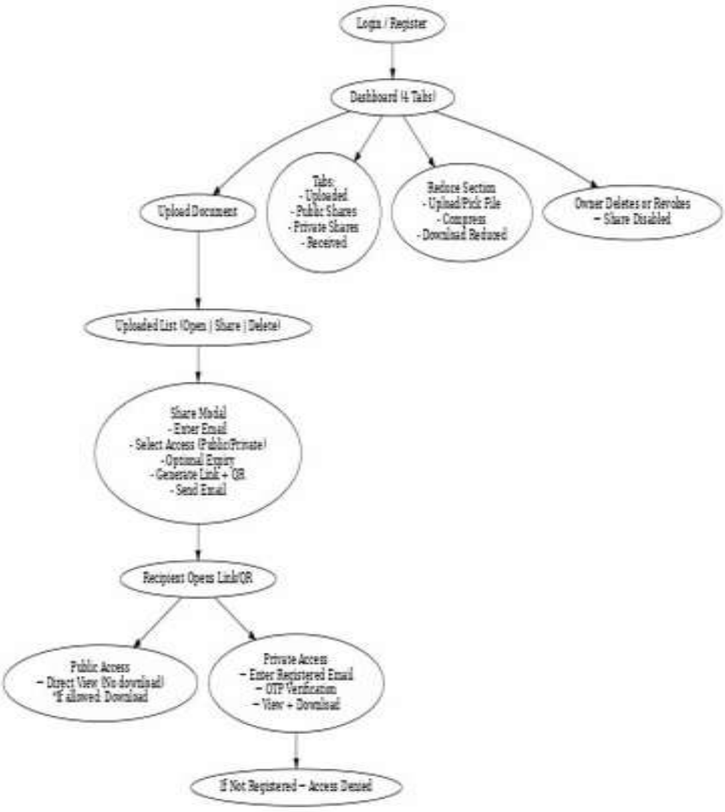

Fig. 1. OTP Verification with QR Codes for a Secure Document Authentication Process.

C. Uploading and Managing Documents

The technology allows users to upload new papers. You can choose to open, distribute, or remove the uploaded files from the list. Additionally, owners have the option to withdraw sharing privileges at any moment, instantly depriving recipients of access.

D. Module for Secure Sharing

The following procedure is carried out when a file is shared:

- The choice between public and private access is made.
- For time-limited access, an optional expiration duration may be specified.
- A QR code and secure link are created.
- The receiver receives an email notification with access details.

E. Flow of Recipient Access

By clicking on the secure link or scanning the QR code, the recipient can access the shared file:

- Public Access: Unless specifically permitted by the owner, recipients can view the material directly without requiring download authorisation.

- Private Access: After entering their registered email address, recipients must verify their OTP. A successful verification process is required before the document can be read or downloaded.
- Access is immediately refused if the recipient is not a registered user.

F. Revocation and Access Control

Dynamic access management is guaranteed by the system. At any point, the owner has the ability to remove the file or remove sharing rights. Revocation stops unauthorised or extended access by rendering the shared link or QR code invalid.

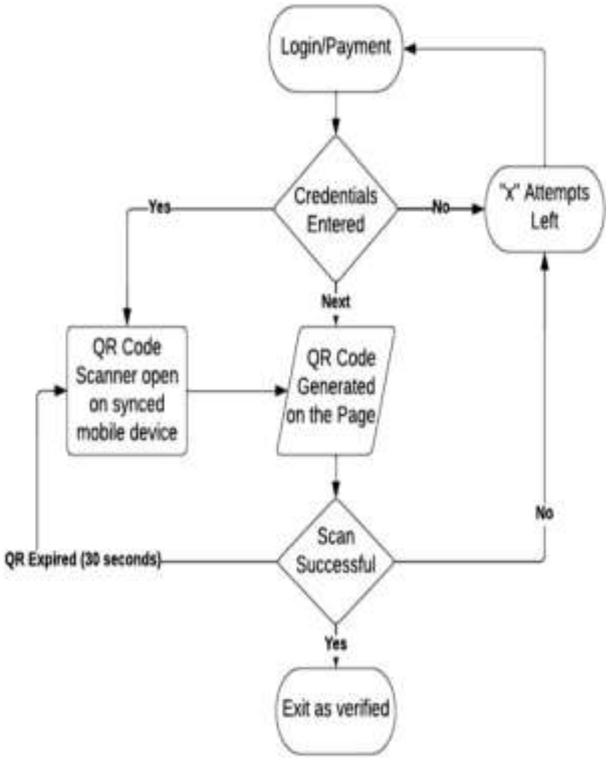

Fig. 2. Sample Data Flow Diagram of the system.

The User and the Authentication Server are examples of external entities in above data flow diagram. Sending an OTP is part of Process 1, which is User Registration/Login. The second step involves uploading a document and creating a QR code (which includes the digital signature of the document). The third step is document download, which involves scanning and validating the QR code. Data stores include the Document Store (documents and their signatures) and the User Database (credentials, OTPs).

VI. DISCUSSION AND RESULTS

By combining QR code technology with OTP-based two-factor authentication, the suggested solution effectively illustrates a safe and effective way to trade documents. To ensure data confidentiality during testing, documents uploaded to the system were encrypted. Time-limited access was made possible using QR codes created specifically for each document, effectively preventing prolonged or unauthorised access. By limiting access to the shared documents to authenticated users, the OTP verification procedure further improved security. Usability was increased by the implementation and successful operation of features including private and public shares, received document management, and document compression. Traceability, accountability, and monitoring of all document interactions were made possible by access logs. All things considered, the system achieved its goals by providing a reliable, easy-to-use, and expandable solution for safe document management in a variety of industries. The system was tested under multiple scenarios, and all functionalities performed as expected:

- Secure login and authentication.
- Document encryption and safe storage.
- OTP-based access and QR verification.
- Secure email notifications.
- Automatic expiry and revocation of shared files.

A secure, user-friendly, and efficient QR-based document sharing system that prevents unauthorized access and ensures safe exchange of sensitive files.

Fig. 3. Document Upload Screen.

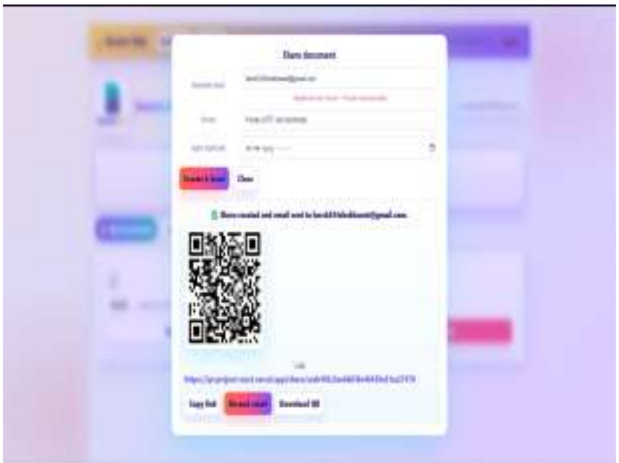

Fig. 4. QR Code Generation Screen.

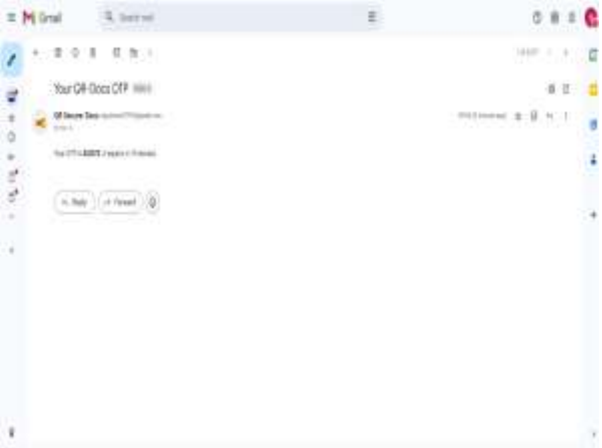

Fig. 5. OTP Verification Popup.

VII. CONCLUSION

The suggested system combines QR code technology with OTP-based two-factor authentication to offer a reliable and secure alternative for digital document sharing. The solution makes sure that only authorized users can access critical data by encrypting documents before sharing them, creating time-limited QR codes, and requiring an OTP for user verification. Usability and productivity are improved by extra features including document compression, private and public sharing, and a centralized dashboard. Accountability is further reinforced by access recording and traceability. All things considered, this integrated strategy provides a dependable, expandable, and intuitive platform that tackles contemporary cybersecurity issues and greatly enhances the protection and administration of digital documents.

VIII. FUTURE WORK

Although the current system successfully provides a secure and efficient way to share documents using OTP verification and QR code authentication, there is still scope for further enhancement and improvement in future versions. In future work, the system can be expanded to include multi-level authentication using biometric verification such as fingerprint or face recognition, which would add an extra layer of security. A mobile application version can be developed for Android and iOS platforms to allow users to upload, scan, and access documents directly through their smartphones. The storage and performance can be improved by integrating cloud platforms like AWS or Google Cloud for faster document access, automatic backups, and scalability to handle a large number of users. The system can also introduce blockchain- based verification for tamper-proof document tracking and history management, ensuring transparency and authenticity of each transaction. Future enhancements may also include an AI- based document classification and search system that automat- ically categorizes uploaded files based on their content or type. Additionally, features like real-time activity monitoring, expiry notifications, file version control, and analytics dashboard can be added to improve user experience and administrative control. Overall, the future development of the system aims to make it more robust, intelligent, and adaptable for use in institutions, organizations, and secure digital document management platforms.

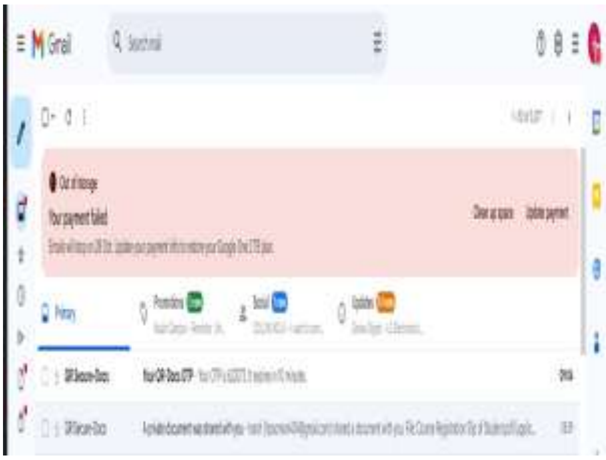

Fig. 6. Email OTP Notification Example.

REFERENCES

REFERENCES

[1] Suhartana, I. K. G., Suputra, I. N. B., Gunawan, A. A. N. G. , "Securing OTP-Based Access in Film-Sharing Platforms Using RSA Encryption and QR Codes" 2023.

[2] Rana, M., Khokale, R., Makesar, M. S., Kakde, V. A., Shende, A. A. ,"Remote File Sharing System for Education Institution"International Journal of Research, 2021.

[3] Nor, F. M., Aziz, S. N. A., Zulkifli, N. A., Nordin, N. A., Yunus, N. S. M, "Laboratory Access Implementing QR Code," International Journal of Computing and Informatics (IJCI),2020.

[4] Patil, V., Katkar, C., Rahate, R., Waykar, S. , "QR Code Document Authentication and Retrieval. Institutional Project Report" MGMCET Kamothe,2024.

[5] Ataelfadiel, M. A. M, "Enhancing Digital Security: A QR Code and OTP-Based E-Authentication System" King Faisal University Research Publication. Available upon request from university repository,2023.

[6] Madhushree, B., Manimegalai, M., Malini, G., “Securing E-Medical Documents Using QR Code,” R.M.K. Engineering College Research Journal. Available upon request or from institutional archive,2022.

[7] Valisireddy, J., Reddy, K. A., Elumalai, R., Mohan, L. N., Anjaneyulu, G. S. G. N,‘Secured Authentication of Online Documents Using Visual Secret Sharing on QR Code,” International Conference on Computing Technologies. Conference Proceedings,2021.

[8] Balaji, S., Pughazendi, N., Praveenkumar, S. E., Vishal, V., Vignesh, R. , “E-Medical Application using QR Code with OTP Generation,” . Institutional Project Report – Panimalar Engineering College,2022.

[9] Inder Pal Singh Sethi, Om Pradyumana Gupta, Sulbha Bhaisare, Ritesh Kumar Dwivedi, Misha Kapoor. ,“An introduction to using QR codes in web portals for synchronizing calendar events over phones” . IAES International Journal of Robotics and Automation, Vol. 13, No. 4, pp. 469–475,2024.

[10] M. Bartłomiejczyk,I. fray ,“Device risk analysis protocol for SMS-based OTP Authentication” ,DOI:10.1109/ACCESS.2024.3445931.

[11] A. A. S. AlQahtani, H. Alamleh and R. Alrawili ,“Privacy-preserving IoT Data Sharing Scheme” ,2022 IEEE 13th Annual Information Tech- nology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2022, pp. 0428-0432, doi: 10.1109/IEMCON56893.2022.9946495.

[12] L. H. A. Reis, M. T. de Oliveira and S. D. Olabarriaga ,“Fine-grained Encryption for Secure Research Data Sharing” ,2022 IEEE 35th International Symposium on Computer-Based Medical Systems (CBMS), Shenzen, China, 2022, pp. 465-470, doi: 10.1109/CBMS55023.2022.00089.

[13] A. Pazienza, E. Lella, P. Noviello and F. Vitulano ,“Analysis of Network-level Key Exchange Protocols in the Post-Quantum Era” ,2022 IEEE 15th Workshop on Low Temperature Electronics (WOLTE), Matera, Italy, 2022, pp. 1-4, doi: 10.1109/WOLTE55422.2022.9882818.

[14] Y. He, X. Jia, S. Zhang and L. Chitkushev ,“EnShare: Sharing Files Securely and Efficiently in the Cloud using Enclave” ,2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Wuhan, China, 2022, pp. 225-232, doi: 10.1109/TrustCom56396.2022.00040.