International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0340
e ISSN: 2584-2854
Volume: 02
Issue: 07 July 2024
Page No: 2354-2358

Secured File Sharing for Xerox Business Model

Prof. Mrs. T. Aparna[1], B. Hima[2], E. Sai Prasanna[3], P. Naga Sravika[4]
[1]Professor, IT, G Narayanamma Institute of Technology and Science, Hyderabad, India.
[2,3,4]Student, IT, G Narayanamma Institute of Technology and Science, Hyderabad, India.
Emails: *aparna.tanam@gnits.ac.in[1], laxmanbakkuru12@gmail.com[2], saiprasannae123@gmail.com[3], sravikasrinivas02@gmail.com[4]*

Abstract
In the Xerox business model aims to share files with net centers without using any accounts. It utilizes a Scanner-like interface to scan QR code associated with the shop name or the particular file sharing session. Once verified, it requests permission to share the specific file, and it gets stored in the shop's cloud storage for a limited time [user defined], after which it is automatically deleted. Here limited time specified by at the time of sharing the file. This approach ensures that no personal data is shared during the file-sharing process, and users can specify unique tags to identify their files. Additionally, the system prohibits taking screenshots to maintain privacy-focused file-sharing method that enhances user confidentiality and prevents unauthorized access to sensitive information.

Keywords: *Expiration Time, Cloud Storage, QR Code.*

1. Introduction
This paper proposes a novel approach to file sharing for Xerox centers [5], leveraging QR code technology and cloud storage integration [1]. In today's digital age, the secure transmission of documents is essential, especially for entities such as Xerox centers that routinely handle sensitive information [3]. Conventional file-sharing methods, including email and messaging platforms, often unauthorized access [4]. To address these challenges, this innovative system eliminates the need for user accounts, streamlining the sharing process while ensuring confidentiality and data integrity. By combining QR codes for initiation and cloud storage for seamless access [6], the system revolutionizes the file-sharing paradigm, offering a secure and efficient solution for Xerox centers [7]. This paper presents the design, implementation, and evaluation of the system, demonstrating its effectiveness in mitigating risks associated with unauthorized access and data breaches. Through this research, we aim to provide Xerox centers with a robust and user-friendly solution for secure document transmission, safeguarding sensitive information in today's digital environment.

2. Literature survey
Farina [1] This approach investigates the process of sharing photos using QR Codes, a widely used digital communication tool. It places special emphasis on improving scalability by integrating online applications and leveraging cloud computing infrastructure. It explores security issues related to cloud-based solutions, emphasizing how crucial it is to preserve data confidentiality and privacy in order to successfully reduce risks. Bharathi [2] By dividing the data into three sections and encrypting each one using a different algorithm—AES, DES, RSA, and LSB steganography—the suggested method improves data security. In addition to strengthening data safety, this hybrid cryptography technique lowers the possibility of a complete data breach in cloud applications. The solution strengthens the overall security posture of the cloud-based environment by reducing the possible impact of key leakage through the diversification of encryption approaches.V. Argyropoulos [3] The newly developed approach ensures that files are stored exclusively on sender and recipient systems by establishing a peer-to-peer, semi-decentralized file

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0340
e ISSN: 2584-2854
Volume: 02
Issue: 07 July 2024
Page No: 2354-2358

sharing architecture. Digital signatures are used as a strong verification tool to assure file integrity. Furthermore, an intuitive browser interface is included to facilitate use and improve usability and accessibility for all users.A Kaushik [4] This investigation looks into using Block chain technology to improve copyright protection programs and address shortcomings in current practices. The strategy attempts to successfully prevent digital piracy by improving license generating operations' integrity and transparency. By ensuring unchangeable records of copyright ownership and license transactions, this creative use of block chain promotes accountability and confidence within the digital content economy.A Menthe [5] In order to greatly improve communication security, the proposal presents a three-layered architecture that integrates steganography, cryptography, and QR Code technology. The system shows strong protective capabilities through a thorough quantitative and qualitative examination against predetermined performance criteria. This novel method effectively mitigates a variety of security risks in digital communication channels while also guaranteeing the confidentiality and integrity of messages.

3. Proposed Work

The proposed system uses state-of-the-art technology to improve security and user control, with the goal of revolutionizing file-sharing behaviours. As information exchanges quickly and widely in the modern digital age, it is critical to protect the integrity and confidentiality of shared documents. Sensitive data is seriously at risk when using traditional file-sharing techniques like email attachments or messaging apps, which are prone to interception and illegal access. We tackle these issues head-on by launching a safe, account-free file-sharing solution that makes use of QR code technology. This novel method prioritizes security, confidentiality, and user convenience while streamlining the sharing process. The technology makes sure that files are only available for a short time by having the sender scan a special QR code to add extra protection by setting expiration time.

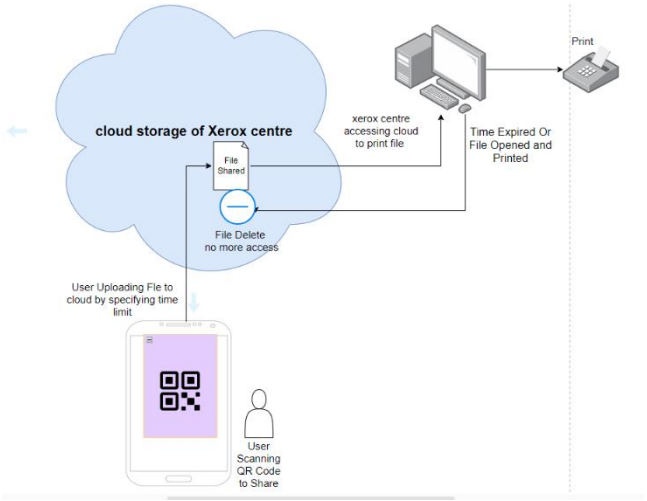

Figure 1 System Architecture

4. Method

Regarding to privacy hazards, this study suggests a novel approach to privacy-preserving file sharing inside the Xerox business model, addressing issues with the dependence of previous techniques on user accounts. Our solution uses QR code authentication and an interface like a scanner to allow safe file sharing without the need for user accounts. When the receiver scans the QR code associated with the sharing session or recipient, the system requests authorization to share the selected file. It then stores the file in the recipient's cloud storage for a predefined period of time, protecting the data. Additionally, users can give files distinct tags to help with categorization. In order to prevent unwanted access, precautions like forbidding screenshots are also put in place, putting user privacy first

4.1 Registration Module

The employees of Xerox use their login credentials to access the web application. After successful authentication, access to their cloud storage is granted. Using a web browser on their device, employees of Xerox access the web application by going to the login page. Entering Credentials, Xerox employees are required to enter their credentials, which normally consist of a username (which is typically an email address) and a password, when they arrive at the login screen. These login credentials are used to confirm the user's identity and establish their degree of authorization on the system Credential

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0340
e ISSN: 2584-2854
Volume: 02
Issue: 07 July 2024
Page No: 2354-2358

Submission: The Xerox staff members submit their information via the online interface by clicking on a certain button, usually labelled "Login" or "Sign in," following the entry of their credentials. Authentication Process, Next the system starts the authentication process, which entails comparing the supplied credentials to user data that has been saved. By confirming the user's identity, this verification establishes whether the user is authorized to use the system. Granting Access, An authentication attempt is considered successful if the user's credentials match those kept in the system's database and the system is accessible to them. The user is thus given access, enabling them to continue using the application.

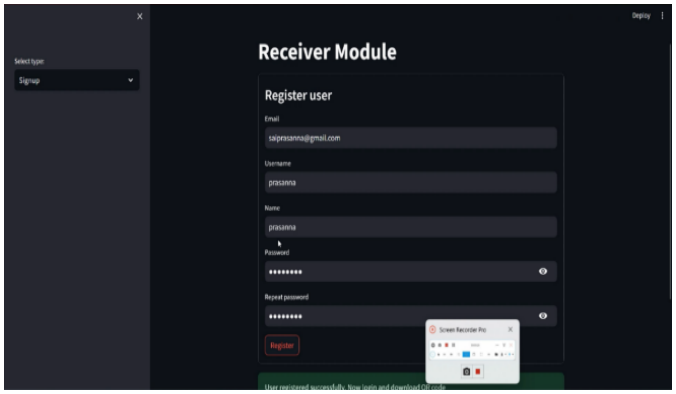

Figure 2 This is the Signup Interface of Xerox Centre Initially He Needs to Sign Up and Download the QR Code

4.2 Scan The Qi Code

Users can enter folder permission codes or scan QR codes to start print tasks. To grant access to the designated folder, the code is verified.

QR Code Scanning: If users want to scan a code, they use their device's camera feature to scan a code linked to the print job or folder they want to print. This QR code might be seen digitally by another device or physically on a document.

Error Handling: When a user enters an invalid or expired code, relevant error messages are sent to them, offering advice on possible debugging techniques or alternate ways to open the folder. browser on their device, employees of Xerox access the web application by going to the login page. Entering Credentials, Xerox employees.

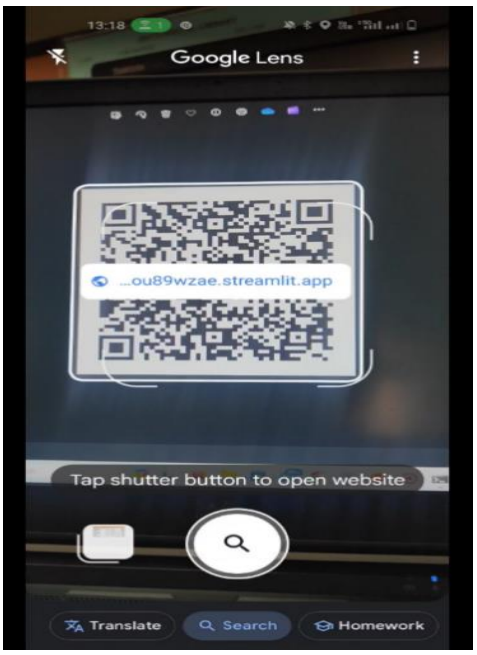

Figure 3 Scanning QR code and Accessing the Link

4.3 File Upload

After choosing files from their devices, users upload them to specific cloud storage folders. The cloud safely stores any files that are uploaded.

Entering a Folder Permission Code: Users also have the option of manually entering a folder permission code that has been given to them. This code acts as the specific folder's unique ID in the cloud storage system.

Verification procedure: The system starts a verification procedure to make sure the supplied code is legitimate as soon as the QR code is scanned, or the folder permission code is input. This check makes sure the user has permission to open the designated folder and start print jobs inside of it.

Access Granting: The user is given access to the designated folder if the code they have provided is successfully compared to the system's data. This enables them to access the contents of the folder for printing and move forward with the print job initiation procedure.

Set expiration time: Users will set file expiration dates, which determine how long a file can be downloaded before it is automatically removed from cloud storage.

Send file: Files sent by users to the Xerox centre are safely transferred to the printing queue at the centre.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0340
e ISSN: 2584-2854
Volume: 02
Issue: 07 July 2024
Page No: 2354-2358

The Receiver Gets the File on His Cloud.Received files are printed by the Xerox centre. When files are printed, users are notified and can retrieve them from their cloud storage.Users that have files with an expiration time selected must download and print them within that time frame else, the contents will be automatically removed from the cloud storage.

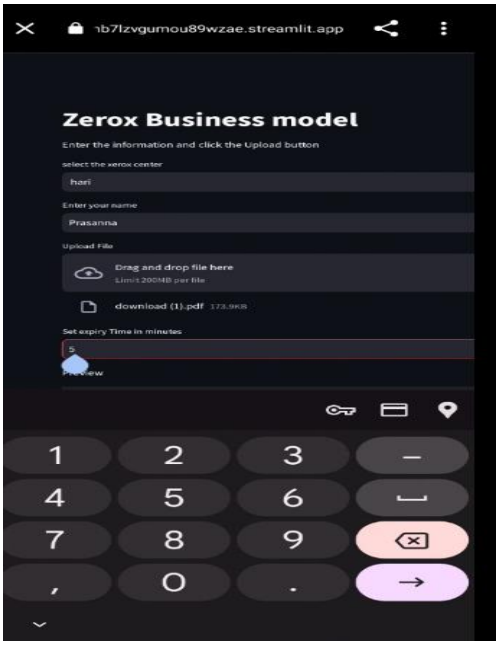

Figure 4 File upload, Setting Expiration Time

4.4 Cloud Storage Integration

The users' cloud storage accounts are smoothly integrated with the file-sharing system, guaranteeing that printed files are automatically synchronized and made accessible from any internet-connected device.

4.5 File Processing At Xerox Center

The Xerox centre prepares the files for printing after it receives them transmitted from the user's cloud storage. Usually, this entails adding the files to the printing queue and adjusting the print parameters like paper size, colour selection, and print quality as needed.

4.6 Printing

The Xerox centre uses its printing apparatus to start the printing process after the files are queued up and prepared for printing. The digital documents are converted into tangible copies when the files are printed onto real paper using the predetermined parameters.

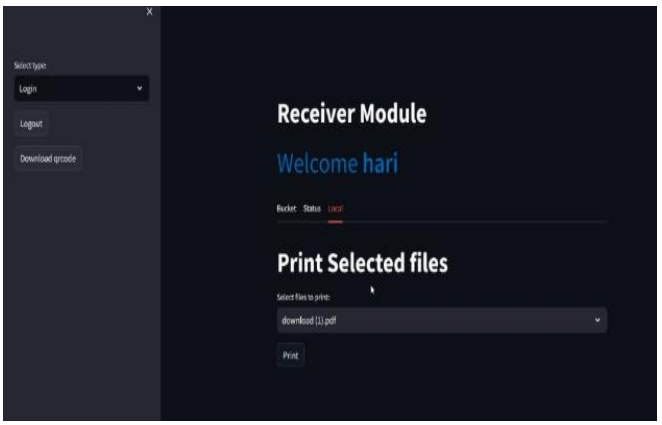

Figure 5 Selecting File to Print and Clicking on Print Results, Hardcopy of File is Seen

5. Result

Overall, the development of a secure and efficient file-sharing system tailored to the specific needs of Xerox centres, leveraging QR code technology to streamline the transmission process and enhance data security for both senders and recipients is done.

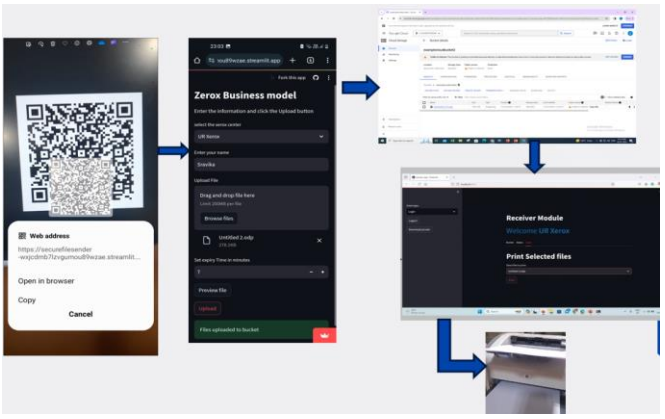

Figure 6 System Snippets

Conclusion

In conclusion, the Xerox business model offers a private and secure method of file sharing without requiring user accounts. It assures that no personal information is shared throughout the sharing process by using a QR code verification system and an interface similar to a scanner. Users can designate special tags for their files, and the system saves them in the cloud storage of the business for a user-specified amount of time. Preventing screenshots improves security and privacy by preventing the collection of passwords. All things considered, this

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0340
e ISSN: 2584-2854
Volume: 02
Issue: 07 July 2024
Page No: 2354-2358

approach puts user privacy first, guards against unwanted access to private data, and provides a reliable solution for safe file sharing.

References

[1]. Farina, N & George, Jossy & Kureethara, Joseph Varghese. (2018). An Image Sharing Technique Using QR Code Through Cloud for Mobile Devices. International Journal of Engineering & Technology. 7. 176. 10.14419/ijet. v7i2.6.10563.

[2]. P. Bharathi, G. Annam, J. B. Kandi, V. K. Duggana and A. T., "Secure File Storage using Hybrid Cryptography," 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatre, India, 2021, pp. 1-6, doi: 10.1109/ICCES51350.2021.9489026.

[3]. V. Argyropoulos, E. Alepis and C. Patsakis, "Semi-Decentralized File Sharing as a Service," 2022 13th International Conference on Information, Intelligence, Systems & Applications (IISA), Corfu, Greece, 2022, pp. 1-8, doi: 10.1109/IISA56318.2022.9904336.

[4]. A. Kaushik and M. Malik, "Securing the transfer and controlling the piracy of digital files using Blockchain," 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT), Sonepat, India, 2022, pp. 324-331, doi: 10.1109/CCiCT56684.2022.00066.

[5]. A. Mendhe, D. K. Gupta and K. P. Sharma, "Secure QR-Code Based Message Sharing System Using Cryptography and Steganography," 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India, 2018, pp. 188-191,

[6]. Suman Srivastava;Snehil Raj, “File Sharing Through Cloud-Based Systems Utilizing Block Chain Technology”2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC).

[7]. Kumar, A., & Verma, G. (2023, December). Secure cloud storage access framework using blockchain technology. In 2023 11th International Conference on Intelligent Systems and Embedded Design (ISED) (pp. 1-5). IEEE.