International Journal of Advance and Innovative Research
Volume 12, Issue 2 (XXI): April - June 2025
ISSN 2394 - 7780

TEMP DRIVE

[1]Roshan Kumar Barnwal, [2]Arif Ali, [3]Akash, [4]Nilesh Kumar, [5]Dr. Pooja Kapoor and [6]Mr. Banarsi Lal Prajapati
[1, 2, 3, 4]Department of Computer Science, MIET, Greater Noida, India
[5]Research Coordinator, Professor, MIET, Greater Noida, India
[6]professor, Department of Computer Science, MIET, Greater Noida, India

ABSTRACT
With the increasing need for secure and private file sharing, traditional cloud storage platforms often require user authentication, leading to privacy concerns. Temp Drive is a novel temporary file-sharing platform designed to allow users to share files securely without login credentials. The platform employs temporary access links, QR codes, and OTP authentication, ensuring a seamless and privacy-focused file-sharing experience. This paper discusses Temp Drive's architecture, key functionalities, security mechanisms, and its potential future enhancements, including AI-based file categorization, blockchain security, and P2P file transfers.

Keywords-- *Temporary file sharing, secure file transfer, privacy, QR authentication, OTP-based access, blockchain security.*

I. INTRODUCTION

In today's digital landscape, file-sharing services play a crucial role in enabling seamless communication, collaboration, and information exchange across individuals and organizations. With the increasing reliance on cloud computing and internet-based storage, users have come to expect convenient, fast, and accessible methods for sharing documents, media, and other digital content. However, most mainstream file-sharing platforms—such as Google Drive, Dropbox, and Microsoft OneDrive—are primarily designed for long-term file storage and collaboration. These platforms require users to authenticate via personal accounts, which involves collecting and storing sensitive user data, including email addresses, access logs, and usage patterns. This inherent requirement raises significant privacy concerns, especially for users who seek a more anonymous or ephemeral method of sharing files.

In contrast, peer-to-peer (P2P) solutions like BitTorrent enable file distribution without a central server, offering decentralization benefits and high transfer speeds. However, such systems generally lack fine-grained control over file lifespan and user access, making them ill-suited for temporary or private sharing scenarios. Furthermore, the persistence of files across distributed networks can pose additional risks related to data leakage and lack of user control over file deletion.

To address these gaps, we propose Temp Drive, an innovative web-based file-sharing platform designed with a core focus on privacy, anonymity, and temporariness. Unlike traditional platforms, Temp Drive eliminates the need for user registration or authentication, thereby reducing the risk of identity tracking and unauthorized data collection. Users can simply upload a file, after which the system generates a secure, time-bound access link and an optional QR code for easy sharing across devices and platforms. After a user-defined expiration period—or after a single download—the file is automatically and irreversibly deleted from the server, ensuring that no residual data is retained beyond its intended usage.

The platform leverages temporary URLs, one-time passwords (OTPs), and encrypted storage to maintain a high level of security while maintaining a minimalist and intuitive user experience. Additionally, Temp Drive's infrastructure is designed to be lightweight, scalable, and API-friendly, enabling future integrations with other tools, mobile apps, or enterprise platforms..

II. LITERATURE REVIEW

File sharing has evolved significantly over the past two decades, becoming an indispensable aspect of modern digital communication and collaboration. Numerous platforms and technologies have been developed to facilitate this process, each with unique trade-offs in terms of usability, scalability, security, and privacy. This section provides a comprehensive overview of existing file-sharing solutions, identifies their limitations, and establishes the motivation for developing a privacy-focused, temporary file-sharing platform such as Temp Drive.

1. Traditional Cloud Storage Services

Mainstream cloud storage providers like **Google Drive**, **Dropbox**, **Microsoft OneDrive**, and **Box** offer robust file- sharing and synchronization features.

ISSN 2394 - 7780

These platforms are widely adopted due to their convenience, support for collaborative workspaces, and integration with productivity suites (e.g., Google Workspace, Microsoft Office 365).

However, these systems typically require **user authentication and persistent storage**, which leads to several privacy-related concerns:

- User data, including metadata and behavioral patterns, is collected and often retained.
- Files remain accessible unless manually deleted by the user.
- Sharing mechanisms rely on email-based permissions, which link activity to identity.

Although these platforms offer features like expiring links or restricted access, they are often buried in advanced settings and still rely on account-based access control. Moreover, **data retention policies** vary across providers, and users must trust these companies to handle their data responsibly.

2. Anonymous File-Sharing Tools

Several anonymous file-sharing tools have emerged to address the privacy limitations of mainstream platforms. Examples include:

- **WeTransfer (free version)**: Allows sending files up to 2 GB without login, with 7-day expiry.
- **Firefox Send** (now discontinued): Offered encrypted file sharing with a limited lifespan and download count.
- **File.io**: Provides ephemeral links for files, which are deleted after a single download or after a specific time.

These services highlight growing user interest in **temporary and secure file sharing**, but many suffer from limitations such as:

- Inconsistent availability (e.g., Firefox Send was discontinued due to abuse concerns).
- Lack of QR code-based sharing for cross-device convenience.
- Limited customization of expiration conditions (time- based vs. download-based).

3. Peer-to-Peer (P2P) File Sharing

Technologies like **BitTorrent** and **Resilio Sync** allow decentralized file sharing without a central server, improving scalability and reducing hosting costs. While P2P systems offer **data redundancy and fault tolerance**, they present the following drawbacks:

- Files are often stored persistently across nodes, making deletion difficult.
- Privacy is limited, as IP addresses of peers are often exposed.
- They are not optimized for **short-term or one- time file exchanges**.

In addition, the requirement for both sender and receiver to be online simultaneously can limit usability in ad hoc sharing scenarios.

4. Security and Privacy in File Sharing

Multiple research studies have explored the security and privacy implications of file sharing. Notable findings include:

- **End-to-end encryption** is critical to ensuring content confidentiality during transmission and storage [Zhou et al., 2018].
- **Temporary authentication mechanisms**, such as OTPs and time-based tokens, can prevent unauthorized access [Wang & Chen, 2019].
- **User anonymity** is increasingly demanded in environments where file origin or identity disclosure could lead to ethical or legal risks (e.g., journalism, whistleblowing) [Greenwald et al., 2014].

However, balancing strong encryption with usability remains a major challenge. Most secure platforms still require users to perform key management or engage in complex configuration processes, which hinders adoption by non-technical users.

5. Emerging Trends and Technologies

Recent advancements open new possibilities for temporary and secure file sharing:

ISSN 2394 - 7780

- **Blockchain** offers tamper-proof records and decentralized file verification [Christidis & Devetsikiotis, 2016], although its application in ephemeral systems is still emerging.
- **Artificial intelligence** can support intelligent file tagging, content filtering, and threat detection [Kim et al., 2021].
- **QR code integration** enhances the ease of cross- device file sharing, particularly in offline or mobile-first contexts.

Despite these innovations, a gap remains for a lightweight, privacy-first platform that:

- Enables **anonymous, temporary file sharing**,
- Uses **time-bound or single-use links**, and
- Offers **intuitive, secure sharing methods** such as QR codes and OTPs.

III. METHODOLOGY

This section outlines the core methodologies employed in the design and implementation of **Temp Drive**, a web- based platform enabling secure, anonymous, and temporary file sharing. The platform is built using a modular architecture with emphasis on privacy, simplicity, and automation. The methodology is divided into key functional modules

1 Temporary File Upload & Sharing

The foundation of Temp Drive lies in enabling users to share files without undergoing any registration or login process. The upload process is handled via a secure front-end interface connected to a cloud-based storage system. The methodology for this process includes:

- **Anonymous Upload Interface**: Users are presented with a drag-and-drop or browse-based upload mechanism on the homepage, with no requirement for user identification.
- **Unique Link Generation**: Upon successful upload, the system generates a unique, randomized **temporary access link** using a secure tokenization algorithm (e.g., UUID or hash-based string).
- **Backend File Mapping**: Uploaded files are mapped to the generated access token and stored temporarily on the server with associated metadata (e.g., upload time, expiration time).
- **Scheduled Deletion**: A background task scheduler (e.g., using cron jobs or serverless functions) automatically deletes files from the system once the set expiration time is reached.

2 Secure Access Mechanisms

To maintain secure access and reduce the risk of unauthorized file downloads, Temp Drive employs multiple access control methods:

- **QR Code Integration**: Along with the temporary link, the system generates a **QR code** that encodes the link, allowing users to easily transfer access across devices or share it physically.
- **OTP-Based Access**: Users can opt to enable **One- Time Password (OTP)** verification, which requires the recipient to enter a time-limited numeric code sent to an email or phone number before accessing the file.
- **Session Tokens**: File access is controlled through **session-based validation**, ensuring that links cannot be reused or cached by third parties. Each file session is logged with a unique temporary token that expires after the download is complete or after a predefined time.

3 Auto-Expiration of Files

To minimize storage usage and ensure data is not stored longer than necessary, Temp Drive integrates a fully automated file expiration and deletion system:

- **Time-Limited File Lifespan**: Users can select a predefined expiration period during upload (e.g., 1 hour, 24 hours, or 7 days). After this period, the file becomes inaccessible.
- **Automatic Deletion Process**: A background service continuously monitors file expiration timestamps and securely deletes both the file and its metadata upon expiry.
- **No Manual Cleanup Required**: This ensures that users do not need to return to the platform to manage or delete previously shared files, enhancing usability and ensuring data hygiene.

ISSN 2394 - 7780

4 System Workflow Summary

1 Upload Phase:
- User uploads a file anonymously.
- System stores file with metadata and creates secure access credentials.

2 Sharing Phase:
- System generates a time-limited link and optional QR code.
- User shares the link or QR code.

3 Access Phase:
- Recipient opens the link, optionally verifies identity via OTP.
- File preview is shown if supported; file can then be downloaded.

4 Expiration Phase:
- File is deleted automatically after the defined expiration period or after a single access, depending on user preference.

IV. TECHNOLOGIES USED

Frontend Technologies
- HTML, CSS, JavaScript
- Bootstrap / Tailwind CSS

Backend Technologies
- PHP for handling server requests.
- Node.js (future integration) for real-time notifications.

Database & Storage
- MySQL for storing file metadata.
- MongoDB (future upgrade) for scalable session handling.
- AWS, Firebase, or DigitalOcean for file storage.

V. FUTURE ENHANCEMENTS & EXPANSION

AI-Based File Categorization
- Uses AI to classify uploaded files into categories.

Mobile App Development
- Dedicated Android & iOS app for seamless file sharing.

Monetization Strategies
- Freemium model with additional features for paid users.

Peer-to-Peer (P2P) File Transfer
- Enables direct file transfers without a central server.

VI. CONCLUSION

In an era where digital privacy and data security are paramount, traditional file-sharing solutions often fall short by requiring persistent user authentication and retaining files indefinitely. This research introduced Temp Drive, a novel, web- based platform designed to address these challenges by enabling temporary, anonymous, and secure file sharing without the need for user registration.

Through a combination of temporary access links, QR code integration, and OTP-based authentication, Temp Drive offers a streamlined, privacy-focused user experience that ensures files are only accessible for a limited period. Its core functionalities—including automated file expiration, session-based retrieval, and online file preview—not only improve usability but also significantly reduce storage overhead and exposure to unauthorized access.

The system's architecture, built on modular and scalable principles, allows for seamless implementation of security features while remaining lightweight and intuitive.

ISSN 2394 - 7780

Additionally, the platform's emphasis on ephemerality and data minimization aligns well with modern privacy standards and user expectations in sensitive or short-term communication contexts.

Looking ahead, Temp Drive holds strong potential for future enhancements. Integrating AI-driven file categorization, blockchain-based file integrity, and peer-to-peer transfer mechanisms could further improve security, transparency, and performance. These advancements would position Temp Drive as a leading solution in the evolving field of secure, temporary file-sharing services.

In conclusion, Temp Drive demonstrates how thoughtful design and minimalism can provide robust privacy and security without compromising user convenience—offering a timely and effective alternative in today's data-conscious digital landscape.

REFERENCES

1. Tilakaratne, S., Jayasuriya, P., Riyaj, S., & Rodrigo, M. (2023). *E-CHEQUE: Re-Defined Era for Financial Transactions*. CORE. Link.
2. Kaur chitranjanjit, kapoor pooja, kaur Gurjeet(2023), "image recognition(soil feature extraction)using Metaheuristic technique and artificial neural network to find optimal output.Eur. Chem. Bull.2023(special issue 6).
3. Maheshwari Chanana shalu, Kapoor pooja,kaur chitranjanjit(2023),"Data mining techniques adopted by google: A study.: Empirical Economics Letters,22(special issue 2).
4. Sukre, A., Fakih, S., Shende, S., Tate, R., & Bendale, S. (2018). *Multi-sharing data using OTP for secure transactions.* Link
5. Mahansaria, D., & Roy, U.K. (2019). *Secure Authentication Using One Time Contextual QR Code for File Sharing and Messaging*. Link
6. Brousek, B.P. (2019). *Multi-Factor Authentication in Large-Scale Secure Systems*. Link