Vol.3 No.2 October 2026: 57-61
International Journal of Computer Science and Humanitarian AI (IJCSHAI)
e-ISSN: 3064-4372
DOI: 110.21512/ijcshaijournal.v3i2.15946

HexDrop: Privacy Preserving, Cross Platform Ephemeral Data Sharing App

Marvin Enrico

Mobile Application and Technology, School of Computer Science,
& Research Interest Group in Education Technology,
Bina Nusantara University,
Jakarta, Indonesia 11480
marvin.enrico@binus.ac.id

Abstract – Online file sharing services is an integral part of modern life. However, existing centralized cloud storage services has several issues in terms of privacy, data breach and data sold to third parties. Furthermore, some of these services are subject to surveillance laws like the CLOUD Act. Existing alternatives such as P2P sharing, lacks cross-platform compatibility and long distance support (over the internet). This paper introduces HexDrop. a unique self-hosted file and data sharing web app that focuses on privacy and ease of use. It uses the seceure TLS protocol and doesn't store the shared data long term where it will delete the data after the sharing session has ended. Since it is web-based, it ensures seamless compatibility across platform. It's ability to be self-hosted on local network also provides additional security against data breaches and unauthorized access compared to centralized cloud services.

Keywords: privacy; self-hosted; ephemeral; security

I. INTRODUCTION

Online file sharing platform, is a web-based service that provides user with the ability to upload, store, retrieve and share digital Files on a remote server that is accessible through the internet. Some of the most used file sharing services are Google Drive, One Drive, Dropbox, etc. However, these platforms have raised significant privacy concerns due to the platform policy and centralized data storage. Google for example, explicitly states in their privacy policy that they collect data for advertisement purposes like showing ads that are correlated to your search history e.g if you search for "smartwatch" on Google search, you might start to see ads for it [1]. Similarly, Microsoft also shares the data they collected to third parties under certain conditions (e.g your privacy settings). They also collect data from their affiliates, subsidiaries and third parties. [2] Microsoft will then use this data to personalize their product, develop existing product, and targeted advertising [3]. In both cases, centralized & corporate controlled cloud storage increases risks of surveillance & exploitation for commerical gains. Data breach is also a worrying concern. According to open source data [4], there were over 22 billion data records exposed in 2019, with the number increasing significantly from 2018.

These kind of data breaches are causing damages in millions (USD) [5] [6] and leaks personal information like phone numbers [7]. Another interesting point is that 30% of these data breaches were linked to third party involvement which further proves that your data were sold to 3rd party [8]. The data obtained from these kind of data breaches are mostly used for illicit purposes like phising and scams calls [9] [10]. Where the criminals will mass call list of phone numbers that they got in the breach. Another way personal data is being utilized, is by being sold to data brokers [11] [12] [13]. Data brokers are individual or a company that collects personal data (such as geolocation, ethnicity, income, political beliefs, etc) from public records or bought privately from other companies that will later be sold again for purposes such as employment, credit or housing. This result in the declining trust of consumer. Furthermore, since those clouds are mostly operating inside United States, they are subject to laws such as the CLOUD act & other legal compliances that allows the government to access users data with a warrant whenever any criminal indication is suspected [14] [15]. Putting data inside public cloud also means that users are putting all of their trust to the competency of the cloud service provider. However, some cloud applications are still vulnerable to attacks especially if it's a high profile

Received: Jun. 02, 2026; received in revised form: Oct 14, 2026; accepted: Oct. 14, 2026; available online: Oct. 29, 2026.

Corresponding: marvin.enrico@binus.ac.id

Copyright © 2026

cloud service provider [16] as there will be a massive amount of public data being stored and is a lucrative target for cyber criminals. There are several methods to deal with this such as using a P2P file transfer protocol and encrypted cloud storages. However, there are usability challenges when we are transferring files to different platforms where users might need to install different apps for each different platform. To address these challenges, this paper aims to provide a solution using a privacy-oriented, self-hosted file and data sharing app that can be locally hosted or be used over the internet with cross-platform support. The shared / uploaded data will be ephemeral and permanently deleted after the user has done sharing their data. The app will use HTTP with TLS protocol which is the most common and safest protocol out there.

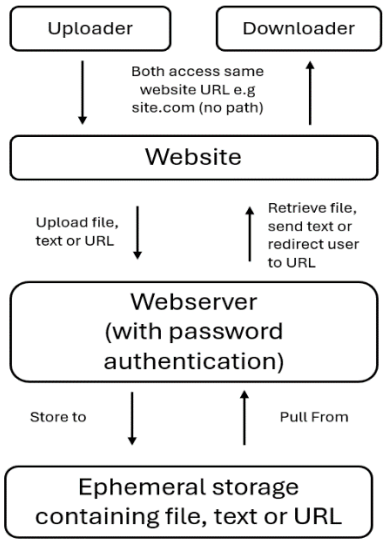

Fig. 1. Web app logic flow diagram

The password authentication will be implemented with a session cookie [17], where the webserver will send a random session ID that is then stored in the user web browser. This session ID will be the identifier used by the webserver to determine whether the user has logged in with the required password or not. The user will also be provided an option to automatically log out after upload as a security measure.

There has been several attempts to address the issue of file-sharing and cloud starge systems. One model is by MEGA.nz. MEGA.nz encrypts the user's data inside the cloud storage using cryptographic key derived from the user's password. Ensuring that even the cloud provider cannot access the uploaded data. However, it is still susceptible to data breach due to the nature of it being a public service. In one case [18], Even though no files were decrypted in the breach, thousand of email addressses and private informations were leaked. This is because MEGA.nz store user data such as emails in a traditional database even though the files that they store are end-to-end encrypted using private key derived from user password that are stored locally [19] as also described in their whitepaper [20]. This incident highlights a critical weakness that public cloud services remain an attractive targe for attackers compared to local/self-hosting solutions.

To mitigate these cloud risks, Peer-to-peer solution like Microsoft's SMB and Apple's Airdrop offers more privacy by eliminating the need of a third party cloud server by sharing files through Wi-fi / Bluetooth connection. However, it is not cross OS/platform compatible and users are still operating within Apple/Microsoft ecosystem, which could still raise privacy concerns. There was also a security vulnerability of phone number leak in the past [21] due to apple using their own custom protocol that is based on bluetooth and privilege escalation vulnerability of SMB [22] instead of using well audited and secure protocol like HTTPS (maintained by non-profit *Internet Engineering Task Force*) [23]. The accident happens because using proprietary / less-reviewed protocol often lack the same level of security scrutiny and testing, making them more prone to security flaws. Outside of Apple's Airdrop and Microsoft's SMB, other local peer to peer file/data sharing app also exists. However, all local peer-to-peer design no matter the protocol is still rather limited due to the requirement of the sender and recipient having to be in the same Wi-fi network / near the other devices via Bluetooth protocol and some devices are still vulnerable to MITM [24] and packet sniffing [25] due to the nature of P2P handshake lacking the root central ceritifcate authority (root CA) infrastructure like what is used in HTTPS where exchanged public keys are verified again by list of trusted public keys by root CA organizations implanted on the user device that forms chain of trust [26]. Due to these limitations explained before, secure and privacy-oriented long distance data sharing with cross platform support remains a challenge to be solved. The author proposes a novel way to share data securely that mitigates all the problem described above via a web server that holds data ephemerally via HTTPS protocol. Furthermore, the app also has a built-in feature to block search engines from indexing the site as a way to prevent accidental exposure of the app to the public by utilizing robots.txt file that search engines will parse before they index the site [27].

The development of the software follows agile SDLC lifecycle [28], this is chosen due to the project compatibility of flexibility, continuous improvement of features while fixing existing bugs at the same time. First, planned features are put into backlog. Then, one of the feature will be worked on and the status will be 'on progress'. After the feature is done, it is then tested for bugs and functionality. If everything goes well, it will then be integrated to the application.

II. PROPOSED METHODS

The app is designed to provide the easiest and fastest way to upload and download data between 2 devices. The app itself is in the form of a web server that can be hosted in local network for internal use or be exposed to the internet for long distance file sharing. Due to the nature of being a web app, it can be used on any OS / platform as long as it has a web browser.

A. Core Features

The web app will support 3 types of data transfer: file, text and URL. After the user upload their data to the web app, the user can access their uploaded data in another device by opening the site again. The site will automatically determine how to send the uploaded data back to the user.

For file uploads, the user can upload files with a "select file" button, drag & drop or Cmd/Ctrl + V. When accessing file uploads, the user can open the site again in the other device and the download will automatically start.

For text uploads, the user can paste the text they want to send into a textbox. When accessing, the user will be provided a "copy text" button that will copy the data to the device clipboard.

For URL upload, the user can paste a valid URL (starting with http:// or https://) to the textbox. When accessing, the user will automatically be redirected to the URL that the user has uploaded before.

B. Internal workings

The server contain an internal state that switches between "upload" and "download" mode. When the user access the web app in "upload" state, the user will be provided a web page to upload their data. After the user upload their data, the internal state will switch to a "download" state. In the "download" state, the user will be provided a web page to access their data that is customized according to the type of data they uploaded (file/text/URL). This method eliminates the need for a unique URL to download the uploaded data and the user can access the same exact web page (e.g. send-data.net) for both uploading and downloading.

C. Security

To protect the web app against unauthorized upload / download from other people / bots, the app contains an optional setting to set a password for both upload and download. The app also contains a feature to automatically log out after uploading in case the user is using a public device to upload their data. The uploaded data is ephemeral in nature and will be deleted after a successful download/access from another device. The app also contains robots.txt file that blocks search engines from indexing the website when it is used over the internet [27].

III. EXPERIMENTAL RESULT

Comparison table can be created based on the explanation and analysis of popular file sharing services, methods and protocols mentioned before.

TABLE I. Comparison Diagram

	HexDrop	Cloud Storage	P2P sharing
Privacy	✓	×	✓
Safer from data breach	✓	×	✓
Cross platform	✓	✓	×
Can be used on local networks	✓	×	✓
Can be self-hosted	✓	×	×
Safe from exploits	✓	✓	×
Safer protocol (HTTPS/TLS)	✓	✓	×
Support URL redirect	✓	×	×
Support text sharing	✓	×	×

Based on feature analysis on the table above, we can conclude that HexDrop is superior compared to cloud storage and P2P sharing based on the feature and benefits that we analyzed. HexDrop is inherently more private because it can be used on local networks (air gapped) and can be self-hosted without relying on 3rd party servers. It is safer from data breach because there is less attack surface when the software is used on local network [29], is not exposed to search engines and uploaded data will be instantly deleted after retrieval. It is web-based which means that it supports cross platform sharing as long as the device includes a web browser unlike P2P sharing that mostly relies on 2 devices having the same protocol (e.g Airdrop). It utilizes the secure TLS protocol that has been used for almost all website on the internet [30] and has features to for URL redirect & instant text sharing that doesn't exist on the alternative.

IV. CONCLUSION

HexDrop is a step forward in a simple, cross-platform data sharing by prioritizing both simplicity and security. By using switch-based web app logic that toggles between download and upload modes, the application removes the necessity of having to manage/share long URLs or account requirement. It's ability to handle mutitide of data types such as file, text and URLs through one place makes it a suitable tool for personal and professional use.

The software is different from traditional cloud storages and P2P protocols through it's decentralized and ephemeral nature. It can be deployed on local air-gapped network or exposed to the internet with password security. It handles data security by immediate termination of data after it

has been accessed and preventing search engine indexing via robots.txt and due to it's web based nature, it is cross platform and compatible with almost all devices.

Ultimately, HexDrop is a simple but robust solution for user who require immediate data transfer with immediate termination of said data and avoid the overhead and issues that comes with third party cloud storage. As the project evolves, features mentioned before such as API support, CLI access and stream-based encryption might allow HexDrop to switch from personal tool to capable for supporting enterprise-level workflow

REFERENCES

[1] Google, "Privacy Policy – Privacy & Terms – Google," *Google.com*, Sep. 16, 2024. https://policies.google.com/privacy (accessed Feb. 28, 2026).

[2] Microsoft, "Microsoft Privacy Statement – Microsoft privacy," *Microsoft.com*, 2024. https://www.microsoft.com/en-us/privacy/privacystatement (accessed Feb. 28, 2026).

[3] "Microsoft Privacy Statement – Microsoft privacy," *Microsoft.com*, 2024. https://www.microsoft.com/en-us/privacy/privacystatement#mainhowweusepersonaldatamodule (accessed Feb. 28, 2026).

[4] N. N. Neto, S. Madnick, A. M. G. D. Paula, and N. M. Borges, "Developing a Global Data Breach Database and the Challenges Encountered," Journal of Data and Information Quality, vol. 13, no. 1, pp. 1–33, Jan. 2021, doi: https://doi.org/10.1145/3439873.

[5] IBM, "Cost of a Data Breach Study," IBM, 2024. https://www.ibm.com/security/data-breach (accessed Feb. 28, 2026).

[6] L. Visakha, "IBM Report: Average cost of a data breach in India touched INR 179 million in 2023," *IBM India News Room*, Jul. 24, 2023. https://in.newsroom.ibm.com/IBM-Report-Average-cost-of-a-data-breach-in-India-touched-INR-179-million-in-2023

[7] "How Your Phone Number is Exposed: Phone Number Leaks," *Global Cyber Security Network*, Nov. 20, 2024. https://globalcybersecuritynetwork.com/blog/how-your-phone-number-is-exposed-phone-number-leaks/ (accessed Feb. 28AD).

[8] Verizon, "2025 Data Breach Investigations Report," *Verizon Business*, 2025. https://www.verizon.com/business/resources/reports/dbir/ (accessed Feb. 28, 2026).

[9] "MSN," Msn.com, 2025. https://www.msn.com/en-in/lifestyle/smart-living/scam-alert-how-do-scammers-get-your-name-mobile-number-and-complete-details-understand-the-whole-story/ar-AA1x6cFI (accessed Feb. 28, 2026).

[10] E. A. Eloksari, "Spam calls, texts frustrate Indonesian consumers," The Jakarta Post, Feb. 15, 2022. https://www.thejakartapost.com/paper/2022/02/24/spam-calls-texts-frustrate-indonesian-consumers.html (accessed Feb. 28, 2026).

[11] Transparency Market Research "Data Brokers Market," www.transparencymarketresearch.com. 2025. https://www.transparencymarketresearch.com/data-brokers-market.html

[12] J. Sherman, "Data Brokers and Sensitive Data on U.S. Individuals Threats to American Civil Rights, National Security, and Democracy," Duke University Sanford School of Public Policy, Durham, North Carolina, 2021. Accessed: 02, 2026. [Online]. Available: https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf

[13] C. Shenkman, S. Bradford Franklin, G. Nojeim, and D. Thakur, "How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers," The Center for Democracy & Technology, Washington, D.C., United States, 2021. Accessed: Feb. 28, 2026. [Online]. Available: https://www.congress.gov/118/meeting/house/116192/documents/HHRG-118-JU00-20230712-SD010.pdf

[14] U.S. Department of Justice, "Criminal Division | CLOUD Act Resources," *www.justice.gov*, Apr. 09, 2019. https://www.justice.gov/criminal/cloud-act-resources (accessed Feb. 28, 2026).

[15] M. Perault and R. Salgado, "Untapping the Full Potential of CLOUD Act Agreements," *Csis.org*, Jun. 06, 2024. https://www.csis.org/analysis/untapping-full-potential-cloud-act-agreements (accessed Feb. 28, 2026).

[16] D. Winder, "Dropbox Warns Hacker Accessed Customer Passwords And 2FA Data," *Forbes*, May 02, 2024. https://www.forbes.com/sites/daveywinder/2024/05/02/dropbox-warns-hacker-accessed-customer-passwords-and-mfa-data/ (accessed Feb. 28, 2026).

[17] Choi, Y. B., L., Y., & LaCroix, K. (2019). Cookies and Sessions: A Study of what they are, how they can be Stolen and a Discussion on Security. *International Journal of Advanced Computer Science and Applications*, *10*(1). https://doi.org/10.14569/ijacsa.2019.0100104

[18] A. Singh, "16 Billion Logins Stolen In Mega Data Breach Threatening Apple, Google And More," *www.ndtv.com*, Jun. 20, 2025. https://www.ndtv.com/feature/16-billion-logins-stolen-in-mega-data-breach-threatening-apple-google-and-more-8712948 (accessed Feb. 28, 2026).

[19] "Transparency," *MEGA*, May 29, 2025. https://mega.io/transparency#what-is-transparency (accessed Feb. 28, 2026).

[20] "Transparency," *MEGA*, May 29, 2025. https://mega.io/transparency#what-is-transparency (accessed Feb. 28, 2026).

[21] A. Heinrich, M. Hollick, T. Schneider, M. Stute, and C. Weinert, "AirCollect," Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Jun. 2021, doi: https://doi.org/10.1145/3448300.3468252.

[22] "Security Update Guide - Microsoft Security Response Center," *Microsoft.com*, 2025. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33073 (accessed Feb. 28, 2026).

[23] "Transport Layer Security (tls)," *datatracker.ietf.org*. https://datatracker.ietf.org/group/tls/about/ (accessed Feb. 28, 2026).

[24] J. Classen and M. Hollick, "Happy MitM," arXiv (Cornell University), Jun. 2021, doi: https://doi.org/10.1145/3448300.3467822.

[25] Z. Wang, "Securing Bluetooth Low Energy: A Literature Review," Harbin University of Science and Technology, Heilongjiang, China. Accessed: Feb. 28, 2026. [Online]. Available: https://arxiv.org/pdf/2404.16846

[26] *Chain of Trust - Let's Encrypt*. (n.d.). Letsencrypt.org. https://letsencrypt.org/certificates/

[27] Google Search Central, "Robots.txt Introduction and Guide | Google Search Central | Documentation," *Google Developers*, 2025. https://developers.google.com/search/docs/crawling-indexing/robots/intro (accessed Feb. 28, 2026).

[28] Hossain, M. I. (2023). Software Development Life Cycle (SDLC) Methodologies for Information Systems Project Management. *International Journal for Multidisciplinary Research*, *5*(5). https://doi.org/10.36948/ijfmr.2023.v05i05.6223

[29] M. Guri, "Mind The Gap: Can Air-Gaps Keep Your Private Data Secure?," *arXiv.org*, 2024. https://arxiv.org/abs/2409.04190 (accessed Feb. 28, 2026).

[30] C. Kerschbaumer, F. Braun, S. Friedberger, and M. Jürgens, "The State of https Adoption on the Web," doi: https://doi.org/10.14722/madweb.2025.23001.