Grenze International Journal of Engineering and Technology, June Issue

D- Protect: A Decentralized Personal Information Vault

Anant Mishra[1], Aabhash Gauda[2], Abhimanyu Singh[3], Anadee[4] and Prof Dr. Kakoli Banerjee[5]
[1-5]JSS Academy of Technical Education/Computer Science, Noida, India
Email: {anantmishra7393@gmail.com, aabhashgauda@gmail.com, Abhimanyusingh.as9198@gmail.com, anadeecs@gmail.com, kakoli.banerjee@jssaten.ac.in}

***Abstract*— D-protect is a safe information management system that puts privacy and control ofdata of its users first. D-Protect uses a decentralized strategy in contrast to conventional password managers by utilizing technologies like Filecoin and IPFS. By never storing or sending your master password, letting users keep control over their data, and continuously keeping data on the Filecoin and IPFS networks, the platform builds trust. D-Protect's open-source design promotes openness and examination, enabling everyone to examine its coding for increased security. Provable ownership, like to cryptocurrency ownership such as FIL or Bitcoin, guarantees consumers complete control over their data.**

***Index Terms*— BCT,Password management, User privacy, Decentralization, IPFS, Filecoin, Opensource, Automated IPFS sync, Unique password generation, SHA- 1 Authentication, Real-time item filtering**

I. INTRODUCTION

In the world of digital D-Protect is a revolutionary in the world of digital security, D-Protect is a revolutionary password management solution that prioritizes user privacy, data ownership and decentralized management. Unlike traditional password managers, D-Protect uses technology combined with IPFS and Filecoin to keep passwords safe and secure, and passwords are never stored or transmitted.Trust is at the core of D-Protect as users have full control over their data, eliminating the need to blindly trust the platform. Its constant connection to the IPFS and Filecoin networks increases data availability, while its open structure allows transparency of the code base.In addition to providing basic password management functions such as automatic IPFS synchronization, password encryption and file storage, D-Protect also brings innovations such as membership, instant filtering and zero-knowledge architecture. D-Protect's emphasis on open source security and encryption methods such as AES256 and SHA-3 represents a revolution in security and user-centered password management, setting a new standard for protecting sensitive information.

A. What makes D-protect better

1) Safe: By never communicating or storing your master password, D-Protect lowers the possibility of unwanted access. D-Protect’s approach to security is fundamentally rooted in safeguarding your valuable information. By adopting a strict policy of never storing ortransmitting your master password, it drastically reduces the chances of unauthorized access. This means that your key to accessing sensitive data remains entirely within your control, minimizing any potential vulnerabilities. This unique method significantly enhances the overall safety of your information. By abstaining from storing or communicating your master password, D-Protect ensures that your data

Grenze ID: 01.GIJET.10.2.47

is shielded from prying eyes or cyber threats. This meticulous attention to security not only meets but exceeds industry standards, providing users with a heightened level of confidence in the protection of their data. With D-Protect, users can rest assured that their critical information remains inaccessible to unauthorized parties. By prioritizing user privacy and employing this stringent security measure, D- Protect stands as a robust and reliable fortress against potential breaches or unwanted access, offering peace of mind in an ever-evolving digital landscape.

2) Trust: Since D-Protect is meant to enable users to independently confirm the security of their data, they do not need to have faith in it. D-Protect operates on a principle that transcends blind trust by empowering users to actively verify the security of their data. Unlike systems that rely solely on user trust, D-Protect is designed to offer transparency and assurance through independent confirmation. By enabling users to personally validate the security measures implemented, D-Protect shifts the paradigm from faith-based reliance to a tangible understanding of security protocols. Users are equipped with the tools and information necessary to confirm the integrity of their data protection mechanisms, eliminating the need for blind trust in the system. This unique approach fosters a sense of empowerment and control among users. They can engage with the system, understand its workings, and verify the security measures in place, ensuring that their data remains safeguarded according to their personal standards and preferences. Ultimately, D-Protect's emphasis on enabling independent confirmation ensures that users don't simply trust the system implicitly but actively

3) participate in and comprehend the security measures, fostering a deeper level of confidence and assurance in the protection of their valuable data.

4) Persistent: Making use of the Filecoin and IPFS networks guarantees data availability over time, improving dependability. Leveraging the Filecoin and IPFS (InterPlanetary File System) networks introduces a layer of persistence and resilience that enhances the long-term availability and dependability of data within D- Protect. Filecoin, as a decentralized storage network, ensures data persistence by employing a unique incentive mechanism. Users' data is distributed across a vast network of storage providers, incentivizing these nodes to maintain and secure the data in exchange for Filecoin tokens. This decentralized approach minimizes the risk of data loss or unavailability, even in the face of hardware failures or network outages, as multiple copies exist across various nodes within the network.

5) Open-Source: D-Protect's open-source design encourages openness by enabling users to carefully examine the coding for assurance of security. D-Protect's commitment to an open-source design empowers users by granting them unprecedented visibility into the system's coding, fostering a culture of transparency, collaboration, and security assurance Through open-source architecture, users gain the ability to scrutinize the codebase thoroughly. This transparency allows for comprehensive examinations by security experts, developers, and the broader community. It goes beyond mere claims of security by offering tangible proof and reassurance through code inspection. This accessibility not only encourages scrutiny but also facilitates collaborative efforts to identify and rectify potential vulnerabilities or weaknesses swiftly. The collective intelligence of a community examining the code enhances the platform's overall security posture, promoting rapid bug fixes and the implementation of robust security measures. Moreover, an open-source approach cultivates trust among users. It serves as a testament to D-Protect's dedication to user security and data privacy, showcasing a commitment to accountability and responsiveness to user concerns. By enabling users to delve into the codebase, D- Protect establishes a collaborative environment focused on continuous improvement and assurance of security standards. This transparency bolsters user confidence, making the platform more resilient, trustworthy, and adaptable to evolving security challenges.

6) Provable-Ownership: Similar to holding cryptocurrency, users maintain ownership of their data, which promotes a sense of security and control. The concept of provable ownership within D-Protect extends beyond data storage; it grants users a sense of sovereignty akin to owning cryptocurrency. This ownership model revolutionizes the perception of data by emphasizing user control, security, and autonomy. Much like owning cryptocurrency, where individuals have direct control over their digital assets without relying on intermediaries, D- Protect ensures that users maintain full ownership of their data. This ownership isn't merely theoretical; it's provable and tangible, enforced through cryptographic principles and decentralized technologies. By implementing cryptographic keys and unique identifiers, D-Protect grants users exclusive control over their data. This means they have the sole authority to access, manage, and dictate the usage and sharing of their information. This sense of control instills confidence, as users know they're not beholden to

external entities for access or management of their valuable data assets. Moreover, this ownership model aligns with the decentralized ethos prevalent in cryptocurrency systems. In D-Protect, users aren't subject to a central authority's whims or vulnerabilities. Instead, they operate within a decentralized framework where their

ownership and control of data are secured by cryptographic protocols, ensuring a higher level of security and reducing the risk of unauthorized access or manipulation. Overall, the provable ownership model championed by D-Protect empowers users, promoting a heightened sense of security, control, and accountability over their data. This paradigm shift redefines data ownership, aligning it more closely with the principles of self-sovereignty prevalent in decentralized digital ecosystems like cryptocurrency. across multiple nodes within the network. Consequently, users can reliably access their data, even if specific nodes are temporarily unavailable. By optimizing the synchronization process, D-Protect harnesses the power of IPFS Sync to bolster data availability and accessibility. This automated approach not only streamlines operations but also fortifies the reliability of data access, ensuring that users can consistently and promptly retrieve their information within the decentralized IPFS ecosystem.

I. DIFFERENCE BETWEEN D-PROTECT AND DIGILOCKER

Features	D-Protect	DIGI Locker
Data Security	Zero-knowledge design,robust encryption	Encryption based securitymeasures
Decentralization	Utilizes decentralized storage networks	May or may not incorporate decentralized features
Password Managemen t	Comprehensive password management features	Password management functionalities
Document Storage	Offers secure document storage	Document storage capabilities
Credit Card Storage	Securely stores credit card information	Handles credit card information securely
Personal Notes	Allows safe storage and management of notes	May or may not include personal note storage
Code Openness	Open-source design for transparency	Level of code openness may vary
Usability	Emphasizes user privacy and data ownership	May have varying user interface experiences
Innovation	Integrates state-of-art technology	May implement innovative security features

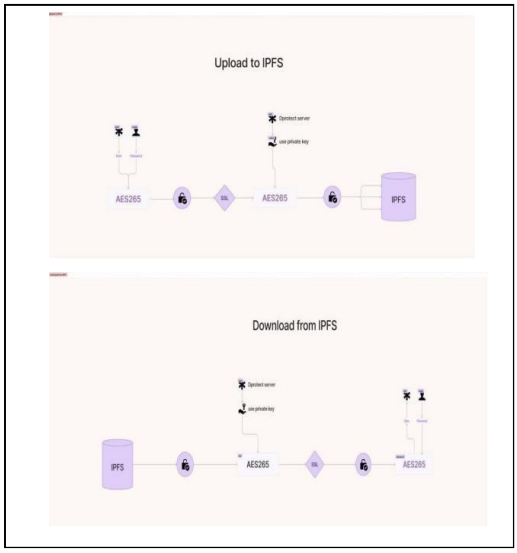

Fig1.1 Internal Working of IPFS

7) Robust and Distinctive Passwords: This enhances security by producing robust and distinct passwords for every website. Generating robust and distinct passwords for every website stands as a cornerstone of modern digital security, greatly fortifying personal and organizational defenses against cyber threats.Robust passwords, created using a combination of upper and lower case letters, numbers, and symbols, significantly heighten the resilience of accounts against brute-force attacks. D-Protect's approach ensures the creation of such strong passwords, minimizing the risk of unauthorized access even if one account is compromised.Moreover, the distinct nature of these passwords enhances security by preventing the domino effect of breaches. Should one site's password be compromised, the uniqueness of passwords generated by D-Protect ensures that other accounts remain unaffected. This compartmentalization strategy drastically reduces the likelihood of widespread hacking incidents that stem from reused or easily guessable passwords.Furthermore, D-Protect's ability to manage these distinct passwords across various platforms and websites simplifies the user experience while fortifying security. Users need not worry about memorizing complex, unique passwords for each site; instead, the system handles this complexity, enabling seamless yet secure access to multiple platforms.In essence, by consistently generating robust and distinct passwords for each website, D-Protect elevates digital security to a new level. This approach mitigates the risks associated with weak or reused passwords, safeguarding sensitive information and bolstering overall cybersecurity posture for users and organizations alike.

8) Document Storage: Expands the platform's functionality by enabling users to safely save documents. Enabling document storage within D-Protect represents a significant expansion of its capabilities, offering users a secure and versatile platform to safeguard a wide array of valuable information.By accommodating document storage, D-Protect transforms into a comprehensive repository that goes beyond password management. Users can securely store a variety of documents, such as legal papers, sensitive contracts, personal records, and more, within the platform's encrypted environment.This functionality streamlines users' digital lives by providing a centralized, secure location for document storage.It mitigates the risk of losing or misplacing critical files, while also offering convenient accessibility from any device with an internet connection.Moreover, the encryption protocols employed by D-Protect ensure that stored documents remain confidential and inaccessible to unauthorized entities. This robust security framework instills confidence in users, assuring them that their sensitive documents are shielded from potential breaches or unauthorized access.Furthermore, the integration of document storage expands D-Protect's utility, making it a versatile tool for personal and professional use. Whether for individuals seeking a secure digital vault for personal documents or businesses requiring a confidential repository for contracts and sensitive information, the document storage feature augments the platform's functionality to cater to diverse user needs.In essence, by incorporating document storage capabilities, D-Protect extends its functionality to become a comprehensive and secure platform for users to not only manage passwords but also safely store and access a wide range of valuable documents, enhancing convenience, security, and peace of mind.

9) SHA-1 Based Password Authentication: This technique adds an extra degree of security by using SHA-1 for password authentication. Using SHA-1 for password authentication adds an additional layer of security by employing a cryptographic hash function that enhances the protection of user passwords within the authentication process.However, it's important to note that while SHA-1 was widely used in the past, it's now considered less secure due to vulnerabilities that have been identified in its hashing algorithm. Over time, as computing power has increased, weaknesses in SHA-1 have been exposed, making it susceptible to certain types of attacks, such as collision attacks.Despite its security limitations compared to more modern hashing algorithms like SHA-256 or bcrypt, implementing SHA-1 within password authentication can still providea basic level of security. It converts passwords into fixed-length hashes, making it computationally challenging for attackers to reverse-engineer the original password from the hash.That said, the use of SHA-1 for password authentication should be approached cautiously. Combining it with additional security measures, such as salting (adding unique random data to each password before hashing) and iterative hashing (applying the hash function multiple times), can mitigate some of the risks associated with SHA-1's vulnerabilities.In an ideal scenario, systems should consider migrating to more secure and robust hashing algorithms like SHA-256 or bcrypt to bolster password security further. While SHA-1 adds an extra layer of security compared to storing plaintext passwords, it's crucial to stay vigilant about evolving security standards and continuously update authentication methods to adapt to emerging threats.

B. Literature Review

1) This chapter delves into the utilization of data-sharing platforms that integrate IPFS Technology, as envisioned by Sun Jianjun. By merging the decentralized attributes of IPFS distributed storage technology, it creates a novel technological landscape for contemporary data exchange.

2) A devised encoding method, established by Ryota Nagaoka, focuses on content-based similarity within IPFS

pointer names. This facilitates the exchange of content in IPFS using SHA-256, a cryptographic hash function. Its purpose is to enable users to recognize content within an IPFS setup akin to an existing file system.
3) An enhanced scheme for a P2P file system is proposed, amalgamating IPFS and Blockchain technologies by Yongle Chen from the Shenzhen Key Lab of Information Theory & Future Network Architecture, among other notable affiliations. This scheme aims to refine the terminology and framework for seamless integration between the two technologies

II. Conclusions

By adopting a decentralized, transparent, and safe methodology, D-Protect transforms the password management industry. It combines state-of-the-art technology with a largefeature set to solve the drawbacks of conventional password managers. In the rapidly changing field of digital security, the platform is positioned as a creative and reliable solution due to its dedication to user privacy, data ownership, and code openness. D-Protect's adoption of a decentralized, transparent, and secure methodology marks a transformative leap in the realm of password management. By integrating cutting-edge technology with an extensive feature set, the platform effectively addresses the limitations inherent in traditional password managers.In a dynamic landscape characterized by ever-evolving digital threats,D-Protect emerges as a pioneering and dependable solution.Its commitment to user privacy,uncompromising data ownership,and transparent code openness positions it as a creative and steadfast response to the challenges of digital security.The platform’s decentralized approach ensures that user data isn't centralized, reducing the vulnerability to single- point breaches commonly associated with traditional password managers. Moreover, its transparency and code openness empower users to verify security measures,instilling confidence in the platform's integrity.By amalgamating state- of-the-art technology with a diverse array of features,D- Protect addresses the shortcomings of conventional password managers.Its dedication to user privacy ensures that sensitive information remains under the user's control, fostering a trust-based relationship between the platform and its users.In essence,D-Protect emerges not just as a solution but as a forward-thinking force in the password management industry.Its commitment to user-centric principles positionsit as a beacon of reliability and innovation, poised to redefine the standards of digital security and privacy in an ever- advancing technological landscape

Acknowledgment

We would like to thank Prof Dr Kakoli Banerjee , our mentor and HOD, for their support and guidance in completing our project on the topic Decentralised Personal Information Vault . It was a great learning experience. I would like to take this opportunity to express my gratitude to all of my group members Abhimanyu Singh , Anant Mishra , Aabhash Gauda , and Anadee. The project would not have been successful without their cooperation and inputs.

References

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
[2] Sankar, L. S., Sindhu, M., &Sethumadhavan, M. (2017, January). Survey of consensus protocols on blockchain applications. In Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on (pp. 1-5). IEEE.
[3] Benet, J. (2014). IPFS-content addressed, versioned, P2P file system. arXiv preprint arXiv:1407.3561.
[4] R.An Introduction to IPFS – ConsenSys – Medium. (2018). Medium. [Online].R.An Introduction to IPFS – ConsenSys – Medium. (2018). Medium. [Online].
[5] Chen, L. (2008). Recommendation for key derivation using pseudorandom functions. NIST special publication, 800,108.
[6] Lemieux, V. L. Blockchain and Distributed Ledgers as Trusted Record-keeping Systems.
[7] 1.N. Yadav, K. Banerjee, and V. Bali, "A survey on fatigue detection of workers using machine learning," International Journal of E-Health and Medical Communications (IJEHMC), vol. 11, no. 3, pp. 1-8, 2020.
[8] 2.T. Sharma, K. Banerjee, S. Mathur, and V. Bali, "Stress analysis using machine learning techniques," International Journal of Advanced Science and Technology, vol. 29, no. 3, pp. 14654-14665, 2020.
[9] 3.K. Banerjee, M. S. Kumar, and L. N. Tilak, "Delineation of potential groundwater zones using Analytical hierarchy process (AHP) for Gautham Buddh Nagar District, Uttar Pradesh, India," Materials Today: Proceedings, vol. 44, pp. 4976-4983, 2021.
[10] 4.K. Banerjee and R. A. Prasad, "Reference based inter chromosomal similarity based DNA sequence compression algorithm," in 2017 International Conference on Computing, Communication and Automation (ICCCA), 2017, pp. 234-238. doi: 10.1109/CCAA.2017.8229806.

[11] K. Banerjee and R. A. Prasad, "A new technique in reference based DNA sequence compression algorithm: Enabling partial decompression," in AIP Conference Proceedings, vol. 1618, no. 1, pp. 799-802, 2014. doi: 10.1063/1.4897025.
[12] K. Banerjee and V. Bali, "Design and Development of Bioinformatics Feature Based DNA Sequence Data Compression Algorithm," EAI Endorsed Trans. Pervasive Health Technol., vol. 5, no. 20, p. e5, 2020.
[13] K. Banerjee, M. B. Santhosh Kumar, L. N. Tilak, and S. Vashistha, "Analysis of Groundwater Quality Using GIS- Based Water Quality Index in Noida, Gautam Buddh Nagar, Uttar Pradesh (UP), India," in Applications of Artificial Intelligence and Machine Learning, A. Choudhary, A. P. Agrawal, R. Logeswaran, and B. Unhelkar, Eds. Singapore: Springer, 2021, pp. 205-212. doi: 10.1007/978-981-16- 3067-5_14.
[14] K. Banerjee, V. Bali, N. Nawaz, S. Bali, S. Mathur, R. K. Mishra, and
[15] S. Rani, "A Machine-Learning Approach for Prediction of Water Contamination Using Latitude, Longitude, and Elevation," Water, vol. 14, no. 5, p. 728, 2022. doi: 10.3390/w14050728.
[16] K. Banerjee et al., "A review on Artificial Intelligence based Sign Language Recognition Techniques," in 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 2195- 2201. doi: 10.1109/IC3I56241.2022.10073000.
[17] K. Banerjee et al., "Prediction of Criminal Behavior Based on Genetic Data - A Review," in2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 2206-2210. doi: 10.1109/IC3I56241.2022.10073062.
[18] K. Banerjee et al., "Assessing Water Quality Index Near Industrial Regions and Aiding in Effective Water Management and Controlling Water Pollution Level," in 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1987-1991. doi: 10.1109/IC3I56241.2022.10073296.