International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Secure Vault – Secure way to store your credentials

Mrs. S. Nandhini
Department of Computer Science and Engineering
Sri Shakthi Institute of Engineering and Technology
Coimbatore, India
nandhiniscse@siet.ac.in

Sudhir R
Department of Computer Science and Engineering
Sri Shakthi Institute of Engineering and Technology
Coimbatore, India
sudhirr22cse@srishakthi.ac.in

Thirunavukarasu A
Department of Computer Science and Engineering
Sri Shakthi Institute of Engineering and Technology
Coimbatore, India
santhoshkumara22cse@srishakthi.ac.in

Viswanathan P
Department of Computer Science and Engineering
Sri Shakthi Institute of Engineering and Technology
Coimbatore, India
viswanathanp22cse@srishakthi.ac.in

Abstract - The Secure Vault Platform is an intelligent file storage and management system designed to enhance digital data organization by integrating AI-powered document analysis, secure access control, and modern web technologies. It streamlines file uploads, sharing, collaboration, and activity monitoring while reducing manual effort in organizing and managing large volumes of documents. The system is built using a robust technology stack consisting of React.js, Go microservices, PostgreSQL, and AI-powered document processing through Google Gemini APIs, ensuring secure data handling, scalable processing, and efficient file management workflows. Through AI-driven document insights, the platform analyzes file content, metadata, and structure to provide automated tagging, duplicate detection, summaries, and contextual understanding. With interactive dashboards for users, secure file sharing features, and real-time storage insights, this system serves as a transformative tool for modern individuals and organizations seeking secure, intelligent, and efficient digital file management solutions.

Keywords - Secure file storage, document management, AI-powered file analysis, secure file sharing, access control, cloud storage platform, intelligent document organization, digital asset management..

I INTRODUCTION

The **Secure Vault Platform** is an advanced digital file storage and management solution designed to modernize and improve the efficiency of handling, organizing, and sharing digital documents. By integrating artificial intelligence, secure authentication, and real-time file management capabilities, the system addresses key challenges in traditional storage environments, where manual file organization, insecure sharing methods, and scattered data locations often create inefficiencies. As digital data continues to grow rapidly across organizations and individuals, there is a growing need for intelligent and scalable tools that provide secure storage, efficient document retrieval, and controlled collaboration. This platform leverages a modern technology stack consisting of React, Go microservices, PostgreSQL, and AI-powered document analysis through Google Gemini APIs to deliver seamless, secure, and efficient file management experiences.

It incorporates AI-driven document analysis mechanisms capable of examining uploaded files to generate intelligent insights such as summaries, automated tagging, and duplicate detection, ensuring organized and efficient document management. Built-in secure sharing and access control features enable controlled collaboration between users, improving accessibility while maintaining strong data protection. Through intelligent processing, the system analyzes multiple aspects of stored documents, such as file content, metadata, structural patterns, and contextual relevance to assist users in understanding and organizing their data. Administrators and users gain access to interactive dashboards that visualize storage usage, file activity, and sharing trends while tracking document interactions over time. Users receive instant AI-generated insights, document summaries, and suggested tags, allowing them to manage and retrieve files more efficiently. With secure authentication, structured data management, and scalable microservice architecture, the platform serves as a reliable and transformative solution for modern digital file storage and management needs.

II LITERATURE REVIEW

[1] J. Biswas, A. Thakur, and P. R. Reddy, *"Secure Cloud-Base File Storage and Management System*," International Journal of Computer Applications, 2022.

This study presents a comprehensive web-based digital management platform that automates key workflows such as user authentication, file uploads, document organization, and secure sharing operations. The authors emphasize the importance of a structured relational database model to manage entities including users, files, metadata, and sharing activities. Server-side logic is used to manage file storage operations and maintain transactional records for auditing and activity monitoring. The study also highlights usability factors such as intuitive upload interfaces and transparent file activity updates to improve user adoption.

[2] K. Sharma and N. Gupta, **"***Web-Based Secure File Storage System with Real-Time Activity Monitoring***,"** IEEE International Conference on Smart Computing and Informatics, 2023. This paper explores the integration of real-time activity monitoring in web-based file storage systems to improve transparency, security, and user trust. The authors demonstrate how continuous file activity updates enable users and administrators to monitor document access, sharing actions, and storage usage. Technical considerations such as data privacy, request handling frequency, and performance optimization are discussed in detail. The research supports the relevance of real-time system monitoring in digital storage platforms and informs future enhancements of our system, particularly in implementing secure and efficient file activity tracking features.

[3] P. Agrawal and R. Singh, **"***Enhancing Digital Storage Systems Using RESTful Web Services,***"** International Journal of Advanced Computer Science and Applications (IJACSA), 2023. This study highlights the role of RESTful web services in building scalable and modular digital storage platforms. The authors explain how APIs enable multiple client applications to access core functionalities such as file upload, document retrieval, and sharing operations without exposing backend logic. Best practices including endpoint versioning, stateless design, authentication, and rate limiting are discussed. The findings strongly support our decision to implement RESTful APIs using Go-based microservices with JWT-based authorization for secure and extensible system integration.

[4] S. Patel and M. Deshmukh, **"***Role-Based Access and Security in Cloud-Based File Management Systems,"* International Conference on Data Science and Security (ICDSS), 2024. This paper examines authentication and authorization mechanisms used in digital storage platforms, with a focus on role-based access control and secure session handling. The authors analyze common security threats and recommend established frameworks such as secure authentication protocols, token-based authorization, and JWT to mitigate risks. Emphasis is placed on restricting administrative privileges and safeguarding sensitive operations like file access, modification, and sharing permissions. This research directly justifies our use of JWT-based authentication and role-based access control mechanisms, ensuring secure, role-aware access control in our system.

[5] L. Zhang, T. Zhao, and Y. Chen, **"***Administrative Dashboards for Effective File Storage and Management Platforms,***"** Journal of Software Engineering and Applications, 2024. This study focuses on the design and effectiveness of administrative dashboards in digital storage systems. The authors identify key features such as user management, file monitoring, access control management, activity tracking, and storage analytics.These insights directly support our integration of centralized administrative interfaces, which provide administrators with unified control and real-time visibility into system operations.

[6] M. K. Das and R. Pandey, **"***Secure Data Handling and Transaction Logging in Web-Based File Management Systems,"* IEEE Transactions on Industrial Informatics, 2023. This paper discusses secure data handling strategies for digital storage platforms, focusing on encryption practices, secure data transfer protocols, and activity logging mechanisms. The authors analyze failure scenarios such as incomplete file uploads, interrupted data transfers, and unauthorized access attempts, and recommend reliable request-handling workflows to maintain system consistency. The findings guide our file management module design, activity logging mechanisms, and administrative monitoring features, ensuring secure and reliable file storage and access management within the secure vault platform.

III PROBLEM STATEMENT

Traditional file storage and document management systems face significant limitations in delivering security, flexibility, and efficient organization within rapidly growing digital environments. Existing platforms often rely on fragmented storage solutions and manual file organization, which restrict user control and reduce efficient collaboration between individuals and teams. Managing documents across multiple storage locations requires users to manually organize, categorize, and retrieve files, often leading to data duplication, misplaced documents, and inefficient workflows. Current storage practices lack intelligent organization, automated insights, and transparent activity tracking, making it difficult for users to manage large volumes of files or understand document usage patterns. The absence of AI-assisted file management further limits productivity and accessibility for users handling complex or large-scale digital data.

Additionally, the lack of modular architecture and scalable integration prevents deeper system extensibility and operational efficiency. Monolithic storage systems and restricted service integration contribute to challenges in scalability, maintenance, and compatibility with modern web-based platforms. Fragmented file metadata, limited administrative visibility, and unclear access control policies make it difficult to monitor system activity or maintain secure document workflows. These limitations highlight the need for a modern, intelligent file storage platform that supports secure access, AI-driven document analysis, efficient sharing mechanisms, and scalable service architecture.

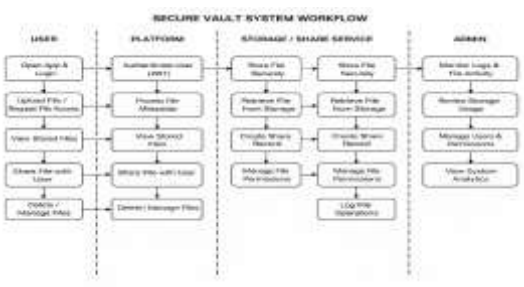

Fig 1.1: Workflow of existing syste

IV PROPOSED SYSTEM

The proposed Secure Vault File Management Web Application is designed to modernize digital file storage and management by providing a secure, scalable, and user-centric platform for storing, organizing, and sharing files. Leveraging intelligent document processing, secure authentication, and structured file workflows, the system enables efficient and transparent management of digital assets. Developed using a full-stack architecture with a React-based frontend, Go microservices backend, and PostgreSQL database, the platform supports secure file uploads, controlled sharing, and efficient document lifecycle management. By incorporating JWT-based authentication for secure access, AI-powered document analysis for automated tagging and insights, and administrative monitoring for centralized control, the system enhances operational efficiency, scalability, and user experience. The platform aims to eliminate manual file organization challenges, improve document accessibility, and deliver a reliable, intelligent, and secure file management solution for individuals and organizations.

V METHODOLOGY

The first stage of developing the Secure Vault File Management Web Application focuses on designing a secure and structured system capable of handling user authentication, role management, and core file management operations efficiently. This begins with defining a robust data model using PostgreSQL to represent key entities such as users, files, file metadata, and sharing records. The application is implemented using a React-based frontend and Go microservices backend architecture, ensuring modular design, scalability, and maintainability. Secure authentication is established using JWT-based authentication mechanisms, which utilize encrypted tokens and secure session validation to protect user credentials. Role-based access control is implemented by identifying user permissions and restricting access to authorized resources, ensuring that users interact only with permitted file operations. Throughout this stage, validation mechanisms are applied to maintain data integrity, prevent unauthorized access, and ensure system reliability.

The next phase focuses on managing the file lifecycle through structured workflows and intelligent processing mechanisms. Users initiate file operations by uploading documents through a secure interface, where the system processes file metadata and stores files within the storage service. AI-powered analysis is applied to examine file content and generate insights such as automated tagging, summaries, and duplicate detection. The system stores file records and manages access permissions based on ownership and sharing rules. Users can securely share files with other authorized users, and access permissions are verified before any document retrieval occurs. The workflow follows a structured lifecycle model, where files move through stages such as upload, storage, sharing, access, and archival or deletion. Each action is recorded with relevant activity logs, ensuring traceability and smooth coordination between system services and users.

In the final stage, the system integrates secure file operations, intelligent processing, and user interaction handling to enhance overall efficiency and usability. The platform utilizes structured API communication between the React frontend and Go microservices backend to enable smooth file uploads, retrieval, and sharing operations while maintaining secure access control. The application also incorporates AI-powered document analysis, allowing users to generate summaries, automated tags, and insights for uploaded files directly through the platform interface. Upon file upload or sharing, the system updates file records and activity logs, enabling further actions such as access monitoring, file management, and permission adjustments. The structured workflow, combined with secure processing and intelligent features, ensures a seamless and reliable file management experience while supporting scalability and future system enhancements.

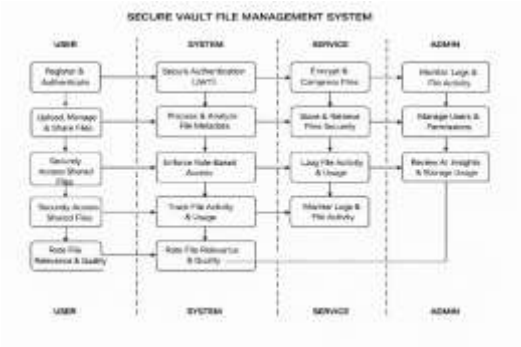

Fig 1.2: Detailed workflow diagram

VI RESULTS AND ANALYSIS

The The Secure Vault File Management Web Application has been successfully developed as a comprehensive and user-centric digital storage platform capable of handling secure file uploads, document organization, controlled sharing, and intelligent document analysis with high reliability and efficiency. The system integrates secure authentication, role-based access control, and structured file management workflows to deliver a transparent and efficient experience for users and administrators. By automating file storage processes, permission management, document retrieval, sharing operations, and activity monitoring, the platform significantly reduces manual effort and organizational complexity compared to traditional file storage methods while ensuring security, usability, and overall system performance.

Fig 1.3: Dashboard Page

The User Dashboard Page allows users to navigate through different sections of the secure file management system and access key features through a centralized interface. It displays important notifications at the top of the page, keeping users updated with file uploads, sharing activities, and system alerts. The dashboard provides an overview of storage statistics such as total files stored, shared documents, and recent activity, along with quick navigation options like My Files, Shared Files, Recent Activity, and Profile for easy access to essential functionalities, ensuring a smooth and user-friendly experience.

Fig 1.4: File Management Page

The Main File Management Interface of the secure vault system enables users to upload and organize files by selecting documents directly from their device, while also allowing users to create folders for better organization if required. It provides real-time information such as file size, upload progress, and storage usage within the user's account. The interface also displays recently uploaded files and shared documents, enabling users to view, manage, and access their stored files efficiently.

Fig 1.5: Shared files page

The My Files Page represents the file management interface of the secure vault system, where users can view both stored and shared documents. It displays each file in a structured format, allowing users to easily track file details and monitor their document activity. For stored files, quick action options such as viewing, downloading, sharing, and deleting are available. The page also shows key details including file name, upload date, file size, and access permissions, while deleted or archived files include the deletion time and the user who initiated the action.

Fig 1.6: Activity Monitoring Page

The Activity Monitoring Page of the secure vault system allows users to monitor real-time updates related to their file operations through an interactive activity interface. It enhances communication by displaying recent actions such as file uploads, downloads, sharing activities, and access requests. Additionally, system notifications are generated to ensure timely updates and smooth coordination when files are shared, accessed, or modified.

Fig 1.7: Storage Page

The Storage Page represents the activity records of the secure vault system, allowing users to view a detailed history of their file operations. It provides complete information for each activity along with options to manage file interactions. Users can view, track, or review actions such as file uploads, downloads, sharing events, and deletions, enabling better monitoring of document usage and system activity.

The User Profile Page of the secure vault system allows users to view and update their personal details, ensuring their account information remains accurate and up to date. It also provides easy navigation to related sections such as File History, Storage Usage, and Shared Files, enabling users to efficiently manage their documents and account activity.

VII CONCLUSION

The Secure Vault File Management Web Application represents a significant advancement in digital storage technology by combining secure authentication, intelligent document processing, and structured file management to deliver a reliable and user-centric storage platform. The system simplifies file uploading, organization, sharing, and monitoring while ensuring security and transparency through well-defined digital workflows.

The platform demonstrated stable performance by accurately handling file operations, secure access control, and system interactions, significantly reducing manual file management efforts and organizational complexity. Secure data handling using Go microservices and PostgreSQL, along with JWT-based authentication and role-based access control, ensured consistency and safety across all operations. Overall, the system provides a scalable, efficient, and secure solution that enhances user experience and establishes a strong foundation for modern and intelligent digital file management systems.

VIII FUTURE WORK

Future enhancements for the Secure Vault File Management Web Application aim to evolve the platform into a more intelligent, scalable, and feature-rich digital storage ecosystem. The system can be extended with advanced AI-powered document analysis and classification to automatically organize files, detect duplicates, and generate deeper insights from stored documents. Advanced analytics based on file activity data can be introduced to generate usage insights, identify storage patterns, and improve overall document management efficiency. Integration of secure and scalable cloud storage services can further improve system reliability, availability, and the ability to handle large volumes of files and users. Additionally, mobile applications for Android and iOS platforms can be developed to increase accessibility and enable users to manage and access their files seamlessly across devices. AI-based document search, intelligent tagging, and contextual recommendations may be incorporated to enhance file retrieval and organization efficiency. Notification services using email and in-app alerts for file sharing, access requests, and activity updates will further strengthen communication. These enhancements will improve scalability, intelligence, and responsiveness, transforming the platform into a more advanced and production-ready secure digital file management solution.

IX REFERENCE

[1] S. Banerjee, R. Johari, and C. Riquelme, “Secure Cloud Storage and Data Management in Distributed Systems,” SIGecom Exchanges, vol. 15, no. 1, 2015. DOI:10.2139/ssrn.2568258

[2] C. Yan, H. Zhu, N. Korolko, and D. Woodard, “Scalable File Storage and Data” Naval Research Logistics, 2020. DOI:10.2139/ssrn.3258234

[3] L. Sun and P. Erftemeijer, “Efficient Data Storage and Retrieval Techniques for Cloud-Based Systems,” Transportation Research Part B, 2019. DOI:10.1016/j.trb.2019.03.008

[4] S. Heydari and E. A. Noughabi, “AI-Driven Data Management and Intelligent File Systems Using Deep Learning Techniques,” SSRN, 2024. DOI:10.2139/ssrn.4746254

[5] P. Kalra, J. Pahwa, A. Sharma, D. Malhotra, and K. Pandey, “Intelligent File Classification and Storage Optimization Using Machine Learning,” International Journal of Scientific Research & Engineering Trends, vol. 10, no. 6, 2024.

[6] Huang, H. L., et al. (2023). Cloud-Based Storage Optimization: Strategies for Scalable Digital Data Management. Highlights in Business, Economics and Management. DOI: (not provided).

[7] Banerjee, S., Johari, R., & Riquelme, C. (2015). Secure Data Storage Models for Distributed Cloud Systems. SIGecom Exchanges, 15(1). DOI:10.2139/ssrn.2568258

[8] MacKay, A. J., & Weinstein, S. N. (2022). Algorithmic Data Management, Privacy Risks, and Regulatory Responses in Digital Platforms. Harvard Business School Working Paper. DOI:10.2139/ssrn.4052431

[9] Alwan, A. A., Ata, B., & Zhou, Y. (2023). Queue-Based Models for Efficient Data Processing and Resource Allocation in Cloud Systems. arXiv. DOI:10.48550/arXiv.2302.02265

[10] Lai, Z., & Li, S. (2022). Spatiotemporal Resource Allocation and Data Distribution in Cloud Storage Networks: A Dynamic Programming Approach. arXiv. DOI:10.48550/arXiv.2206.03298

[11] Tang, X., Zhang, F., Qin, Z., et al. (2021). Unified Learning Frameworks for Intelligent Data Management Systems. arXiv. DOI:10.48550/arXiv.2105.08791

[12] Lu, K., & Du, H. (2024). Decision Models for Data Storage Platforms Considering Network Effects and Resource Optimization. 36(1), 147-163. DOI:10.7307/ptt.v36i1.320

[13] Bai, J. (2024). User Behavior and Data Management Strategies in Cloud-Based Digital Platforms. Economics & Management Studies, 4 (Issue). DOI: (not provided).

[14] Kalra, P., Pahwa, J., Sharma, A., Malhotra, D., & Pandey, K. (2024). Machine Learning Approaches for Intelligent Document Classification and Storage Systems. Int. Journal of Scientific Research & Engineering Trends, 10(6). DOI: (not provided).

[15] Mejjaouli, A., & Tadj, L. (2023). Adaptive Resource Allocation Strategies for Cloud-Based Data Storage and Service Systems.E–Commerce Research. DOI:10.3390/0718-1876/20/3/224