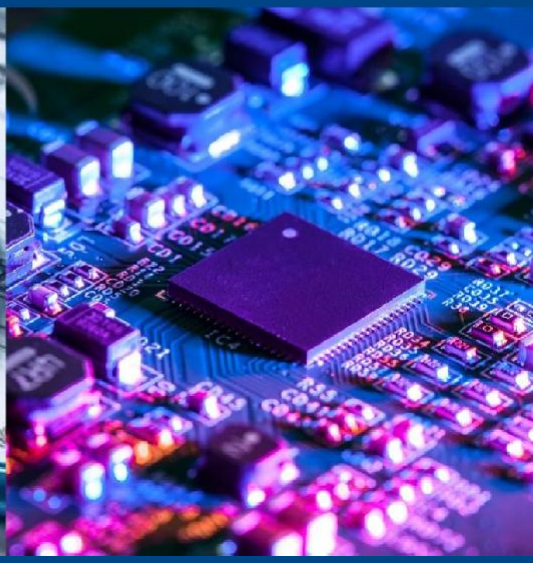
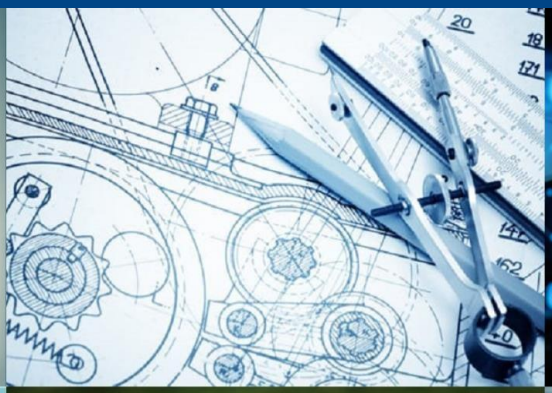
ISSN: 2582-7219

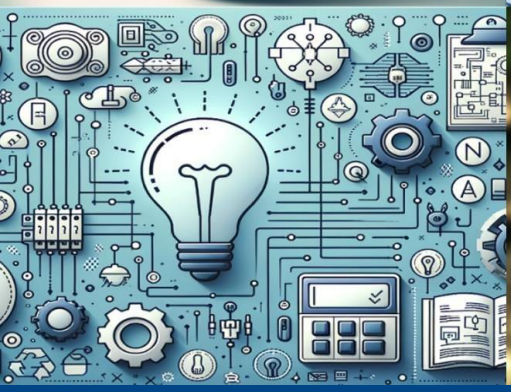




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 8, August 2025

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808059

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

SECURE COLLAB: ENCRYPTED WORKSPACE FOR FILE SHARING & TEAM COLLABORATION

Dr.M S Shashidhara, Deekshitha V

Professor & HOD, Department of MCA, AMC Engineering College, Bengaluru, India

Student, Department of MCA, AMC Engineering College, Bengaluru, India

ABSTRACT: Secure Collab is a complete, real-time program that helps with sharing files and documents, making it easier for people to work together from a distance. It was made with the idea that workplaces are often remote, so file and document sharing can be done easily without worrying about security or unauthorized access. The program allows workspace creators to invite collaborators through a notification system and assign them roles like Creator (Creator), Editor, or Viewer. This ensures proper access control while encouraging smooth collaboration with other users in a shared workspace. Secure Collab solves many common problems in remote settings, such as communication interruptions, lack of central control, and security threats from data breaches. To give a clearer idea, Secure Collab is built with several important features: (i) it stores all files securely in encrypted format, and (ii) it has role-based access control. Designed with a focus on user experience and ease of use,

Secure Collab improves productivity and supports teamwork in distributed environments. It is also a scalable solution for educational institutions, businesses, and teams working across multiple locations. Secure Collab not only changes the way file sharing and collaboration work but also strengthens an organization's control over digital content in a safe and user-friendly environment. Keywords: file sharing, collaboration, role-based access, workspace, secure platform.

I. INTRODUCTION

As we live in the digital age, remote and flexible work styles are becoming more common. Teams now depend on online tools to collaborate effectively, but using multiple disconnected applications often creates confusion, miscommunication, and difficulties in managing access. Secure Collab addresses these challenges by providing a single, unified platform where users can share files, assign tasks, and work together in real time. The platform allows workspace creators to manage participants by assigning roles such as Creator, Editor, or Viewer, ensuring proper access control and smooth collaboration among all members. With features like encrypted file storage, role-based access, Secure Collab keeps teamwork secure, transparent, and well-organized. It reduces the need to switch between different tools, improves overall productivity, and ensures that all team members work from the same space in a reliable and efficient manner.

II. LITERATURE SYRVEY

[1] P. Bharathi et al., “Hybrid cryptography-based secure file storage in cloud,” 2021. https://ieeexplore.ieee.org/document/9507132
[2] S. Arora and P. K. Atrey, “SecureC2Edit: A Secure Collaborative Document Editing Platform,”2024 https://ieeexplore.ieee.org/document/10323461
[3] M. Liu et al., “Cloud-edge collaborative storage system for cost and delay reduction,” 2024. https://ieeexplore.ieee.org/document/10325177
[4] S. Thukral et al., “User engagement analysis on online discussion platforms: A study of Reddit,” 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8711355
[5] K. Yamamoto and T. Hirotsu, “A secure multi-platform file sharing framework,” 2022. https://ieeexplore.ieee.org/document/9752341
[6] B. S. Rawal and S. S. Vivek, “Encryption-based file sharing models: A review,” 2017. https://ieeexplore.ieee.org/document/8251759

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808059

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

EXISTING SYSTEM

Most existing collaboration tools, such as Google Drive, Dropbox, and Microsoft Teams, provide cloud storage, document sharing, and basic access control. While these platforms allow real-time editing and communication, they operate as separate applications, requiring users to switch between multiple tools for file sharing, discussions, and task management. This results in scattered information, reduced productivity, and inconsistent permission handling. Moreover, current systems often lack fine-grained, workspace-level role management and integrated security features like end-to-end encryption across all collaboration activities.

PROPOSED SYSTEM

The proposed system, Secure Collab, provides a unified and secure workspace for file sharing and collaboration. Unlike existing tools, it integrates encrypted file storage, real-time sharing, and role-based access control within a single platform. Workspace creators can invite members and assign roles such as Creator, Editor, or Viewer to ensure proper authorization. The system also includes notifications and discussion features to support smooth communication. By combining collaboration, security, and access management, Secure Collab reduces dependency on multiple disconnected tools and offers a scalable, user-friendly solution for teams working in distributed environments.

III. SYSTEM ARCHITECTURE

The Secure Collab architecture consists of four main architecture layers: Presentation Layer, Business Layer, Service Layer, and Data Access Layer. Having this structure ensures the applications are organized, maintainable, and scalable for secure workspace activities that may be done individually or collaboratively.

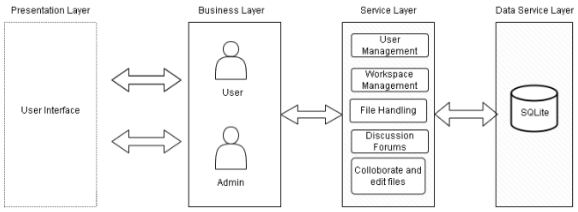


Fig 3.1 System Architecture

[1] Presentation Layer: The presentation layer acts as the interface in front of the platform that ensures all users can utilize the platform without disruption. In the presentation layer, there are entry points to core functions that include management of folders, navigation of workspaces, and collaboration. The layer will be developed for user-ability and communicates directly with business logic to present the most up to date, real time data.

[2] Business Layer The business layer defines and governs core roles for the platform - User and Creator. Users only interact with folders, files and conversations that occur in workspaces - Creators oversee a lot more as they control user management, monitor activity, and manage workspace- wide settings. Role-based access controls provide confidence that the activities users conduct is dependent upon rights and responsibilities while simultaneously safeguarding sensitive actions and data.

[3] Service Layer The service layer is the core functionality of Secure Collab and consists of modular services that include the following: User Management, which consists of registration, authentication, and permissions based on role. The Workspace Management service, which deals with creating, editing, and organizing workspaces. The File Management service, which manages the upload of files, edit files and the organization of files such as folders and subfolders. The Discussion Forums to carry out written collaborative dialogue and communications in workspaces. Collaborate and Edits Files allow users to collaborate online and share real-time online files.

[4] Data Service Layer At the heart of our data persistence is the SQLite database. The database manages storing user data, workspace metadata, files, and discussion threads. This layer communicates directly to the service layer to maintain integrity and security of data, while users perform read/write activity, allowing the service layer to primarily maximize read/write with lightweight deployment options.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. METHODOLOGY

The development of Secure Collab followed a structured and iterative approach to ensure functionality, security, and scalability. The process began with requirement analysis, where the core needs of encrypted file sharing, workspace creation, role-based access control, and real-time discussions were identified, along with non-functional requirements such as security, usability, and scalability. Based on these, a layered system design was created, separating the presentation, business, service, and data layers. The presentation layer focused on user interaction, the business layer enforced roles and permissions, the service layer managed collaboration modules, and the data layer ensured encrypted storage using SQLite.

The database schema was designed to store users, workspaces, roles, files, and logs in a secure relational model. Encryption was applied to sensitive data to maintain confidentiality and integrity. Implementation was carried out in stages, beginning with authentication and role assignment, followed by encrypted file handling, workspace management, and the addition of discussion forums and notifications. Finally, audit logging was integrated for accountability.

Testing was performed throughout the development cycle, covering functionality, integration, and security. The system was validated against unauthorized access and performance issues, ensuring stability under multiple users. After successful testing, the platform was deployed in a secure environment with monitoring to maintain reliability.

V. DESIGN & IMPLEMENTATION

The design of Secure Collab is guided by the principles of modularity, security, and scalability. The system adopts a layered architecture that separates the user interface, business logic, collaboration services, and data storage, ensuring maintainability and robust performance.

A. System Design

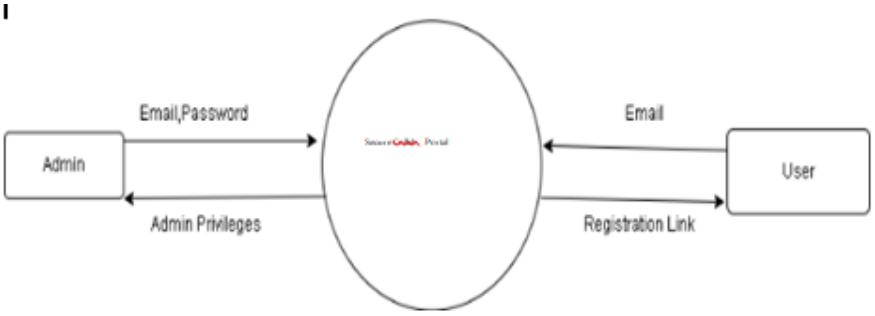
The overall design of Secure Collab is represented using the Context Diagram, where the central system interacts with two main external entities: Creator (Creator) and User.

Presentation Layer: Provides an intuitive user interface that enables workspace creation, file upload, role assignment, and real-time collaboration.

Business Layer: Defines participant roles such as Creator (Creator), Editor, and Viewer, ensuring that each action performed is aligned with the assigned privilege.

Service Layer: Contains the major collaboration services, including User Management, Workspace Management, File Handling, Discussion Forums, and Collaborative Editing.

Data Service Layer: Uses an SQLite database to store encrypted files, user credentials, workspace details, and activity logs, ensuring confidentiality and integrity.



B. Implementation

The implementation of Secure Collab was carried out in iterative stages to ensure continuous validation and improvement.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

User Authentication: Creators authenticate with email and password, while users join via registration links sent through notifications.

Role-Based Access Control (RBAC): Each workspace enforces access levels —Creator manages the workspace, Editors modify content, and Viewers have read-only privileges.

Encrypted File Storage: All uploaded files are encrypted before storage, preventing unauthorized access even at the database level.

Collaboration Features: Users can edit, share, and discuss files within their workspace, supported by real-time notifications.

Database Integration: SQLite is used for secure, lightweight storage of user data, files, and logs. Security Mechanisms: Encryption ensures data confidentiality, while centralized role management minimizes risks of data breaches.

VI. OUTCOME OF RESEARCH

The development of Secure Collab resulted in a functional and secure collaboration platform that successfully combines file sharing, role-based access control, and encrypted storage within a unified environment. The system provides a workspace model where creators can invite participants, assign roles, and manage collaboration with greater control. Unlike existing solutions, Secure Collab integrates discussions, notifications, and file management into a single platform, reducing the need to switch between multiple tools.

The outcomes of the research demonstrate that the platform ensures confidentiality through encryption, transparency through audit logging, and flexibility through role assignments.

Functional testing confirmed that only authorized users could access files, while performance evaluation showed that the system supports multiple users without significant delays. By addressing security threats such as unauthorized access and data breaches, Secure Collab enhances trust in digital collaboration.

Overall, the project validates that a secure, role-based, and user-friendly platform can improve productivity in remote and distributed environments. The research outcome shows that Secure Collab is not only technically feasible but also practical for adoption in educational institutions, organizations, and enterprises seeking a reliable collaboration solution.

VII. RESULT AND DISCUSSION

The Secure Collab platform was successfully implemented and tested in a controlled environment with multiple users. The results show that the system performed efficiently, with smooth navigation, quick response times, and secure handling of file operations. Users were able to register, create workspaces, upload and share encrypted files, and participate in discussions without encountering major issues. Role-based access control worked as intended, ensuring that only authorized users could perform actions such as editing or viewing files.

Security testing confirmed that unauthorized access was effectively blocked, and data confidentiality was preserved through encryption at both storage and transmission levels. The notification system and discussion forums helped

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

reduce communication gaps, allowing team members to remain updated in real time. Performance testing further indicated that the platform could handle multiple users simultaneously without significant delays, validating its scalability.

In comparison to existing tools, Secure Collab eliminates the need for switching between separate applications for storage, communication, and access management. By combining these features into a single secure platform, the system improves efficiency and enhances trust in collaborative work environments. The discussion highlights that Secure Collab not only meets its intended objectives but also provides a practical and scalable solution for modern organizations.

VIII. CONCLUSION

The implementation of Secure Collab has shown that a unified platform for encrypted file sharing and team collaboration can effectively overcome the challenges faced in remote and distributed work environments. The system provides a secure workspace where creators can invite participants, assign roles, and manage collaboration in real time. By combining features such as role-based access control, encrypted storage, notification services, and integrated discussion forums, the platform ensures both productivity and data protection. Testing confirmed that the system enforces access restrictions correctly, preventing unauthorized actions while allowing seamless interaction for authorized users. The use of encryption at storage and transmission levels further strengthens the confidentiality of shared information. Compared to conventional tools that require multiple applications for storage, communication, and permission management, Secure Collab offers a streamlined and reliable solution in a single environment. Overall, the project demonstrates that secure collaboration is not only achievable but can also be made simple and user-friendly. Secure Collab can be adapted for use in enterprises, educational institutions, and organizations of varying sizes, supporting safe and efficient teamwork.

REFERENCES

[1] "Secure File Storage Using Hybrid Cryptography," Putta Bharathi; Gayathri Annam; Jaya Bindu Kandi; Vamsi Krishna Duggana; Anjali T., (IEEE), 2021.
[2] "SecureC2Edit: A Framework for Secure Collaborative and Concurrent Document Editing," Shashank Arora; Pradeep K. Atrey, (IEEE), 2024.
[3] "Collaborative Storage for Tiered Cloud and Edge: A Perspective of Optimizing Cost and Latency," Mingyu Liu; Li Pan; Shijun Liu, (IEEE), 2024.
[4] "Analysing Behavioural Trends in Community Driven Discussion Platforms Like Reddit," Sachin Thukral; Hardik Meisheri; Tushar Kataria; Aman Agarwal; Ishan Verma; Arnab Chatterjee,(IEEE), 2018.https://ieeexplore.ieee.org/document/8508687
[5] "File system to support secure cloud-based sharing," Kensho-Yamamoto; Toshio-Hirotsu,(IEEE), 2022.https://ieeexplore.ieee.org/document/10070678
[6] "Secure Cloud Storage and File Sharing," Bharat S. Rawal; S. Sree Vivek, (IEEE), 2017.https://ieeexplore.ieee.org/document/8118422

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com