

CITADEL – Personal Digital Security Vault

S. Nandhini, M R. Kanishka, T. Kanishka, K S. Kanishk, R S. Kanisha

Department of Computer Science and Engineering, Sri Shakthi Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India

Published October 2026

Abstract

CITADEL is a Personal Digital Security Vault developed to securely store and manage users' sensitive digital information in one centralized platform. In today's digital world, people manage multiple passwords, website accounts, important documents, and private information. Storing these details in different places can make them difficult to organize and protect. CITADEL provides a secure digital vault for managing website credentials, important documents, and private notes. It includes features such as password generation, password strength checking, search, and categorization for convenient management. User authentication and appropriate security mechanisms help protect the stored information from unauthorized access. The system is designed with a simple and attractive interface that makes navigation easy for users. The project will initially focus on developing the frontend interface and user experience. Backend and database integration will be added to provide secure storage and complete functionality. Overall, CITADEL aims to provide a convenient, organized, and secure environment for managing personal digital information.

Keywords: CITADEL; personal digital security vault; password management; data encryption; secure document storage; user authentication; password generation; information security; privacy protection; digital asset management

1 Introduction

In today's digital world, people use numerous websites, mobile applications, and online services for communication, education, banking, entertainment, and professional activities. These services require users to manage multiple passwords, account credentials, important documents, and other sensitive personal information. Storing such information in different locations, such as notebooks, mobile devices, and separate applications, can make it difficult to organize, retrieve, and protect. Weak passwords, repeated password usage, and improper storage practices can also increase the risk of unauthorized access and data exposure. Therefore, an organized and secure approach is required to manage personal digital information efficiently.

CITADEL is a Personal Digital Security Vault developed to provide a centralized platform for storing, organizing, and managing users' sensitive digital information. The proposed system brings together password management, secure document storage, private notes, and password generation within a single application. Instead of maintaining confidential information across multiple locations, users can access their stored information through one organized interface. CITADEL aims to improve convenience, accessibility, and security by providing a structured environment for managing different types of personal digital data.

Password management is one of the major components of CITADEL. Users often maintain multiple accounts across different websites and applications, making it difficult to remember individual login

credentials. Reusing the same password across multiple accounts can increase security risks if one account becomes compromised. The Password Vault module allows users to store and organize credentials such as application names, usernames, email addresses, and passwords. It also supports managing multiple accounts associated with the same application, allowing users to maintain separate login details for personal, academic, and professional purposes.

Secure document management is another important feature of the proposed system. Individuals frequently need to maintain digital copies of identity documents, academic certificates, personal records, and professional files. Keeping these documents in different folders or storage locations can make retrieval inconvenient and increase the possibility of accidental exposure. CITADEL provides a Secure Document Locker that allows users to upload, categorize, and manage important digital documents in a centralized location. Features such as document search, categorization, viewing, downloading, and deletion help users organize their files and access them whenever required. Appropriate security mechanisms are intended to protect confidential documents from unauthorized access.

The system also includes a Private Notes module for storing sensitive information that may not belong in the password or document categories. Users can maintain personal reminders, confidential notes, and other important information within their digital vault. Organizing passwords, documents, and private notes in separate modules improves the overall structure of the application. A search facility and category-based organization can further help users locate specific information without manually checking multiple files or records. These features make CITADEL a convenient platform for managing different forms of personal information.

Password generation and password strength checking are additional components designed to improve users' security practices. Weak and predictable passwords can make online accounts more vulnerable to unauthorized access. The Password Generator allows users to create strong passwords by selecting options such as password length, uppercase letters, lowercase letters, numbers, and special characters. The Security Center can evaluate stored passwords and identify potential weaknesses, including weak or reused credentials, where these checks are implemented. By providing security recommendations, the system encourages users to adopt stronger password practices and improve the protection of their online accounts.

User authentication and data protection are essential aspects of CITADEL. Since the application handles confidential information, access must be restricted to authorized users. The proposed system includes a registration and login mechanism to manage user access. Passwords used for authentication should be stored using an appropriate password-hashing algorithm rather than as plain text. Sensitive information that must be retrieved later, such as stored account passwords, requires suitable encryption and secure key management. These security measures are intended to reduce the risk of unauthorized access and protect the confidentiality of users' information.

CITADEL also focuses on providing a simple, attractive, and user-friendly interface. A clear dashboard presents an overview of the user's digital vault and provides convenient access to important features, including the Password Vault, Document Locker, Private Notes, Password Generator, Security Center, Activity History, Trash, and Settings. The dashboard can display summary information about stored items and the overall security status of the vault. Additional features, such as activity monitoring and deleted-item recovery, can improve transparency and help users manage their information more effectively when supported by the implementation.

The proposed system follows a modular development approach in which the frontend interface, backend services, and database are integrated to provide complete functionality. The frontend is responsible for displaying the application interface and handling user interactions. The backend processes application requests, manages authentication, and coordinates secure data operations. The database stores the information required by the system, while suitable encryption mechanisms protect sensitive data. This separation of responsibilities improves the maintainability and scalability of the application and provides a foundation for future enhancements.

In addition, CITADEL is designed to support the management of digital information throughout its lifecycle. Users can add, search, update, categorize, and delete stored information according to their requirements. A Trash and Recovery module can allow deleted items to be restored within a defined recovery period, helping prevent accidental data loss. Activity History can record important operations performed within the application, while Settings can provide options for managing account preferences and security configurations. Together, these features aim to provide a more organized and controlled digital information management experience.

In conclusion, CITADEL provides a centralized approach to personal digital security by combining password management, secure document storage, private notes, password generation, and security monitoring within a single platform. By integrating user authentication, appropriate encryption, organized data storage, and an intuitive interface, the system aims to simplify the management of sensitive digital information while improving security and accessibility. The proposed application can be useful for students, professionals, and individuals who manage multiple online accounts and important personal documents. Through further development and testing, CITADEL aims to provide a reliable and convenient environment for protecting and managing personal digital information.

2 Literature survey

The increasing use of websites, mobile applications, and online services has created a growing need for secure management of personal digital information. Users often manage multiple passwords, online accounts, confidential documents, and private information across different platforms. Storing these details in separate locations can make them difficult to organize and protect. Conventional methods, such as writing passwords in notebooks or storing documents in unprotected folders, may expose sensitive information to unauthorized access. Recent developments in cybersecurity, encryption, password management, and secure data storage have encouraged the development of centralized digital vault applications. CITADEL aims to address these challenges by providing a single platform for securely storing and managing personal digital information.

2.1 Password management systems

Password management systems help users store and organize login credentials for different websites and applications. Managing multiple passwords manually can be difficult and may encourage users to reuse weak passwords. A centralized password vault helps users retrieve credentials whenever required. CITADEL provides a Password Vault for storing and organizing login details. It also supports managing multiple accounts associated with the same application.

2.2 Data encryption and secure storage

Data encryption protects sensitive information by converting readable data into a protected format. Authentication verifies a user's identity before allowing access to confidential information. These

techniques are essential for applications that store passwords and personal documents. CITADEL is designed to use appropriate encryption and authentication mechanisms. These security measures aim to reduce unauthorized access and protect stored user information.

2.3 Password hashing and user authentication

Password managers help users store and organize login credentials for multiple websites and applications. CITADEL provides a Password Vault that allows users to manage passwords, search credentials, and maintain multiple accounts for the same application.

2.4 Secure document storage

Digital document management systems help users store, organize, and retrieve important files efficiently. Personal documents, academic certificates, and identity records require appropriate protection. Keeping files in different locations can make them difficult to manage and access. CITADEL provides a Secure Document Locker for uploading and categorizing important documents. Search and file-management features help users retrieve and manage their documents conveniently.

2.5 Password generation and security analysis

Strong passwords help protect online accounts against unauthorized access. Password generators create complex passwords using letters, numbers, and special characters. Password strength analysis can identify weak or reused credentials and encourage better security practices. CITADEL includes a Password Generator that allows users to customize password requirements. Its Security Center is designed to provide password-strength information and recommendations.

2.6 Private notes and information retrieval

Private notes applications allow users to store confidential information, reminders, and important personal details. Without proper organization, retrieving stored information can become time-consuming. Search and categorization features improve information accessibility. CITADEL provides a Private Notes module alongside its password and document management features. This integration allows users to manage different types of personal information within one application.

2.7 Database management and data protection

Database management systems provide efficient methods for storing, updating, and retrieving application information. Secure database access is important when handling confidential user records. Appropriate access controls and encryption can help protect sensitive information. CITADEL uses a database-backed architecture to manage user accounts and vault data. The integration of frontend, backend, and database components supports organized information management.

2.8 Limitations of existing systems

Existing applications may require users to manage passwords, documents, and private notes through separate platforms. This can increase the effort required to organize and retrieve personal information. Weak authentication and inadequate data protection can also create security risks. CITADEL aims to address these limitations by combining essential digital security features into one platform. The system focuses on improving convenience, organization, accessibility, and protection of personal digital information.

3 Proposed methodology

3.1 User registration and authentication

CITADEL allows users to create an account using their name, email address, and master password. The login system verifies user credentials before granting access to the vault. Secure authentication mechanisms help prevent unauthorized access to personal information.

3.2 Password vault management

The Password Vault allows users to store and manage passwords for different websites and applications. Users can save usernames, passwords, and account details in one place. Multiple accounts for the same application can be stored separately, making them easier to identify and manage.

3.3 Secure document storage

The Document Locker allows users to upload and organize important files, such as academic certificates, identity documents, and personal records. Documents can be arranged into categories for easy access. Search, viewing, and downloading options help users manage their files conveniently.

3.4 Private notes management

The Private Notes module allows users to store confidential information and personal reminders. Users can create, edit, view, and delete notes whenever required. Keeping notes inside the digital vault helps organize important information in one location.

3.5 Password generation

The Password Generator helps users create strong passwords for their online accounts. Users can select the password length and include letters, numbers, and special characters. This feature encourages users to avoid weak and easily guessed passwords.

3.6 Security analysis

The Security Center helps users understand the strength of their stored passwords. It can identify weak or reused passwords and provide suggestions for improving security. These recommendations encourage users to follow better password management practices.

3.7 Search and categorization

CITADEL provides search and filtering options to help users find passwords, documents, and notes quickly. Information is organized into separate categories based on its type. This reduces the time required to locate specific records.

3.8 Activity history

The Activity History module records important actions performed within the vault, such as logins, password additions, and document uploads. Users can review available activity records and timestamps. This feature improves transparency and helps users monitor the use of their vault.

3.9 Trash and recovery

The Trash module temporarily stores deleted passwords, documents, and notes when recovery is supported. Users can restore accidentally deleted items or permanently remove unwanted information. This feature helps reduce accidental data loss.

3.10 Dashboard and settings

The dashboard provides an overview of stored passwords, documents, notes, and security information. Users can quickly access the main features from one place. The Settings module can provide options to manage profile details, change the master password, and configure additional security features.

3.11 Backend and database integration

The frontend provides the interface, while the backend processes user requests and manages application operations. The database stores the information required by the system. Appropriate encryption, secure password hashing, and access controls help protect sensitive information.

3.12 Testing and validation

CITADEL is tested to ensure that its features work correctly and securely. Testing includes login, password management, document uploads, note creation, search, and recovery operations. Security testing also checks authentication and whether users can access only their own information.

3.13 Overall methodology

CITADEL combines password management, document storage, private notes, password generation, and security monitoring in one digital vault. Its simple interface helps users organize and retrieve information conveniently. The proposed system aims to improve the security, accessibility, and management of personal digital information.

4 System implementation

The implementation of the CITADEL Security Vault focuses on developing a secure and user-friendly platform for managing passwords, personal documents, private notes, and other confidential information. The system provides a centralized digital vault where users can store and retrieve their important information whenever required. A key feature of CITADEL is its ability to manage multiple accounts belonging to the same website or application, allowing users to identify and access each account separately.

The frontend is designed as a web-based interface that allows users to interact with the different modules of the application. The dashboard provides access to the Password Vault, Document Locker, Private Notes, Password Generator, and Security Center. The interface is organized to make storing, searching, updating, and retrieving information simple and convenient.

The backend manages user authentication, data processing, and communication between the frontend and the database. It handles operations such as saving passwords, managing documents, updating private notes, and retrieving stored records. Encryption techniques are used to protect sensitive information, while authentication mechanisms help prevent unauthorized access to the vault.

The Password Vault allows users to store login credentials for different websites and applications. Users can save usernames, passwords, account names, and related details. When an application has multiple accounts, CITADEL keeps their information organized separately. This makes it easier to identify the correct account without confusion.

The Document Locker provides a central location for managing important digital files, such as academic certificates, identity documents, and personal records. The Private Notes module allows users to store confidential information and reminders. Additional features, such as password generation, search, categorization, and security analysis, help users manage their digital information more efficiently.

The system integrates the frontend, backend, and database to provide a complete information management workflow. The application is designed with a modular structure so that additional security features and management tools can be included in future versions. CITADEL aims to simplify personal information management while improving data organization, accessibility, and protection.

4.1 Hardware requirements

The hardware requirements for CITADEL are moderate because users can access the application through a standard computer with a modern web browser. Backend processing and database operations can be performed on a local system or a suitable server environment.

- **Processor:** Intel Core i3 or higher
- **RAM:** Minimum 4 GB; 8 GB recommended
- **Storage:** Minimum 256 GB HDD or SSD
- **Display:** Standard laptop or desktop display
- **Internet:** Stable internet connection for online database and deployment access

4.2 Key considerations

- Smooth execution of the web application
- Efficient processing of user requests
- Secure storage and retrieval of personal information
- Reliable communication between frontend and backend
- Sufficient storage for application files and uploaded documents

Users can access CITADEL through a laptop or desktop computer using a supported web browser. The exact requirements may vary depending on the deployment environment and the size of the stored data.

4.3 Software requirements

CITADEL uses web development technologies, backend services, and database tools to provide password management and secure information storage.

- **Frontend:** HTML, CSS, JavaScript, and the framework used in the project
- **Backend:** Node.js and Express.js
- **Programming Language:** JavaScript
- **Database:** MongoDB Atlas or MongoDB
- **Data Protection:** AES-256-GCM encryption for sensitive data, where implemented

- **Authentication:** Secure login and session or token-based authentication, according to the implementation
- **Development Tool:** Visual Studio Code
- **Testing Tool:** Web browser and API testing tools
- **Version Control:** Git and GitHub
- **Deployment:** A suitable hosting platform for the frontend and backend

These tools provide the development environment required to build, test, store, and manage the information handled by CITADEL. The final list should match the technologies actually used in the project.

4.4 Software description

CITADEL is a web-based personal security vault designed to help users manage confidential digital information through a centralized platform. It combines password management, document organization, private notes, and supporting security features in one application.

- User registration and login
- Password storage and management
- Multiple accounts for the same application
- Secure document storage and organization
- Private notes management
- Password generation
- Search and categorization of stored information
- Security analysis of stored passwords, where implemented
- User profile and settings management
- Backend and database integration

The backend processes requests received from the frontend and communicates with the database to store or retrieve information. Sensitive information should be protected using appropriate encryption and access-control mechanisms. User authentication helps ensure that each user can access only their own vault data.

The dashboard provides a simplified view of the application's main modules. Users can navigate between passwords, documents, notes, and other available features without using separate applications for each type of information. Search and categorization options help users locate specific records more quickly.

The system is designed with a modular architecture, allowing new features to be added without redesigning the entire application. Future improvements may include multi-factor authentication, encrypted backups, additional security notifications, and enhanced recovery options.

CITADEL aims to provide a convenient and organized way to manage personal digital information. Its main objective is to reduce the difficulty of handling multiple accounts and important records while maintaining appropriate security and privacy. The effectiveness of the system depends on correct implementation, secure configuration, and testing of its protection mechanisms.

5 Advantages

The main advantages of CITADEL are as follows:

- **Centralized Information Management:** Stores passwords, important documents, and private notes in one place, making personal information easier to organize and manage.
- **Multiple Account Management:** Allows users to store multiple accounts for the same website or application separately, helping them identify and access the correct account easily.
- **Improved Data Security:** Uses appropriate security mechanisms to protect confidential information and reduce the risk of unauthorized access.
- **Secure Password Storage:** Provides a centralized Password Vault where users can store and manage login credentials for different websites and applications.
- **Strong Password Generation:** Helps users generate strong passwords using combinations of letters, numbers, and special characters to improve account security.
- **Secure Document Management:** Allows users to store and organize important files, such as academic certificates, identity documents, and personal records in one location.
- **Private Notes Storage:** Provides a dedicated space for storing confidential notes, reminders, and other important personal information.
- **Easy Information Retrieval:** Provides search and categorization features that help users locate specific passwords, documents, and notes quickly.
- **User-Friendly Interface:** Offers a simple and organized dashboard that helps users navigate between different modules without difficulty.
- **Reduced Information Loss:** Centralizes important digital information and, where backup or recovery features are available, helps users recover accidentally deleted or lost records.
- **Improved Accessibility:** Allows users to access and manage their stored information through the application's supported interface whenever required.
- **Scalable and Flexible:** Can be extended with additional features, such as multi-factor authentication, encrypted backups, and security notifications, according to future requirements.
- **Efficient Account Organization:** Keeps login details organized by application, website, and account name, reducing confusion when managing several online accounts.
- **Privacy Protection:** Uses appropriate authentication, access controls, and encryption techniques to help maintain the confidentiality of users' personal information.
- **Future Expandability:** Supports the addition of new modules and security improvements as user requirements and technology evolve.

6 Result and analysis

The CITADEL Security Vault provides a centralized platform for managing passwords, personal documents, and private notes. It helps users organize their digital information and manage multiple accounts belonging to the same application separately.

The system integrates the frontend, backend, and database to support efficient information storage and retrieval. Features such as password generation, document management, and search options help users manage their personal information conveniently. Appropriate security mechanisms help protect confidential data from unauthorized access.

Overall, CITADEL aims to simplify digital information management by combining essential features in a single platform. It improves organization, accessibility, and convenience while emphasizing the security and privacy of users' personal information.

Screenshots of the main pages and modules of the implemented system are shown in Figures 1–12.

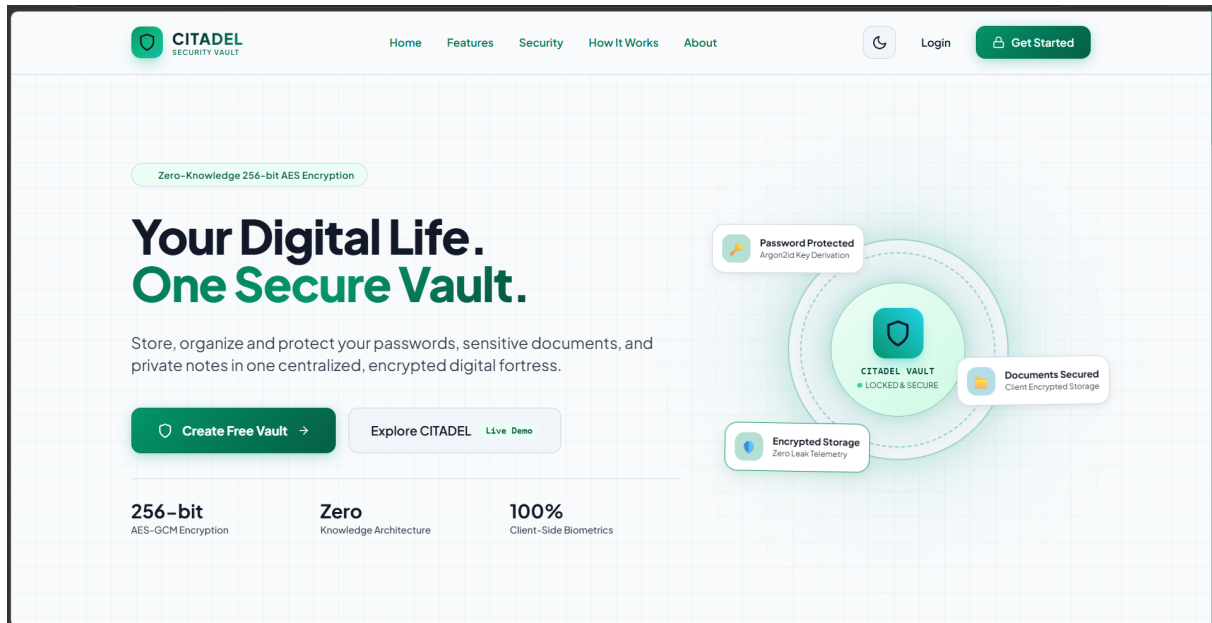


Figure 1. Landing page of CITADEL.

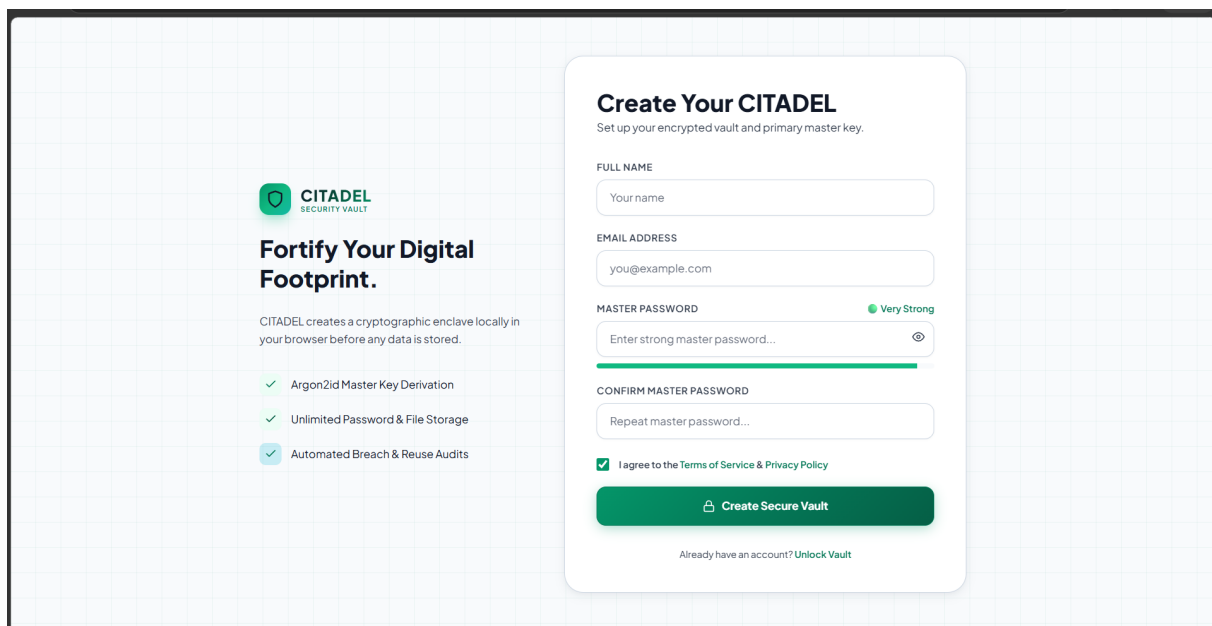


Figure 2. Account registration page.

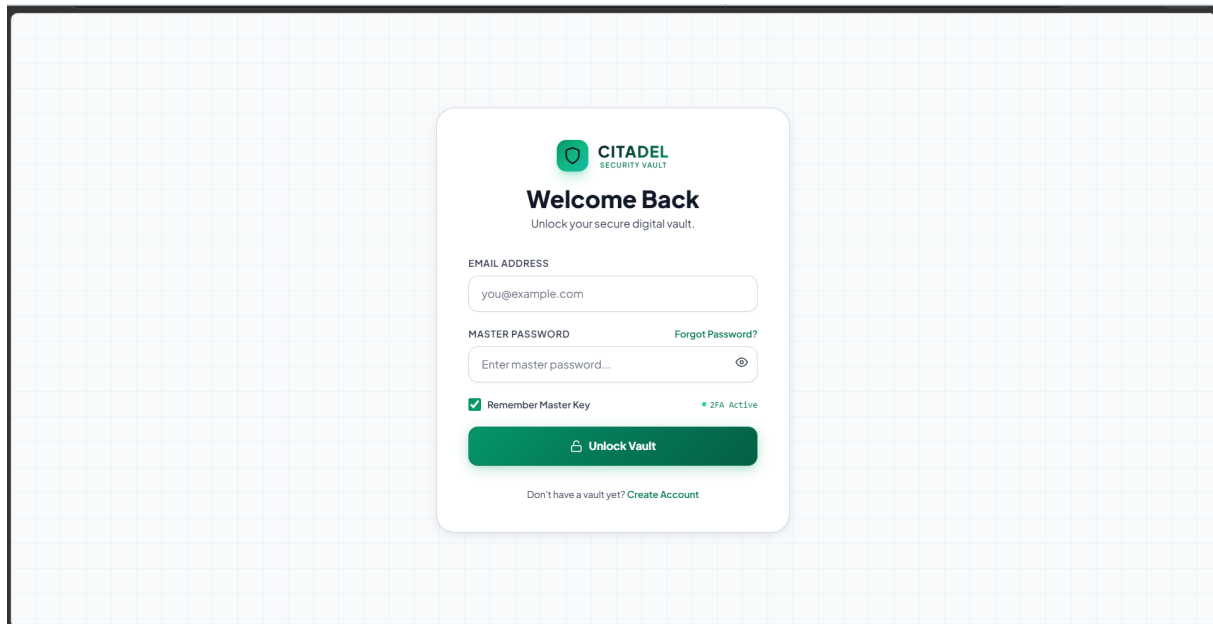


Figure 3. Login (unlock vault) page.

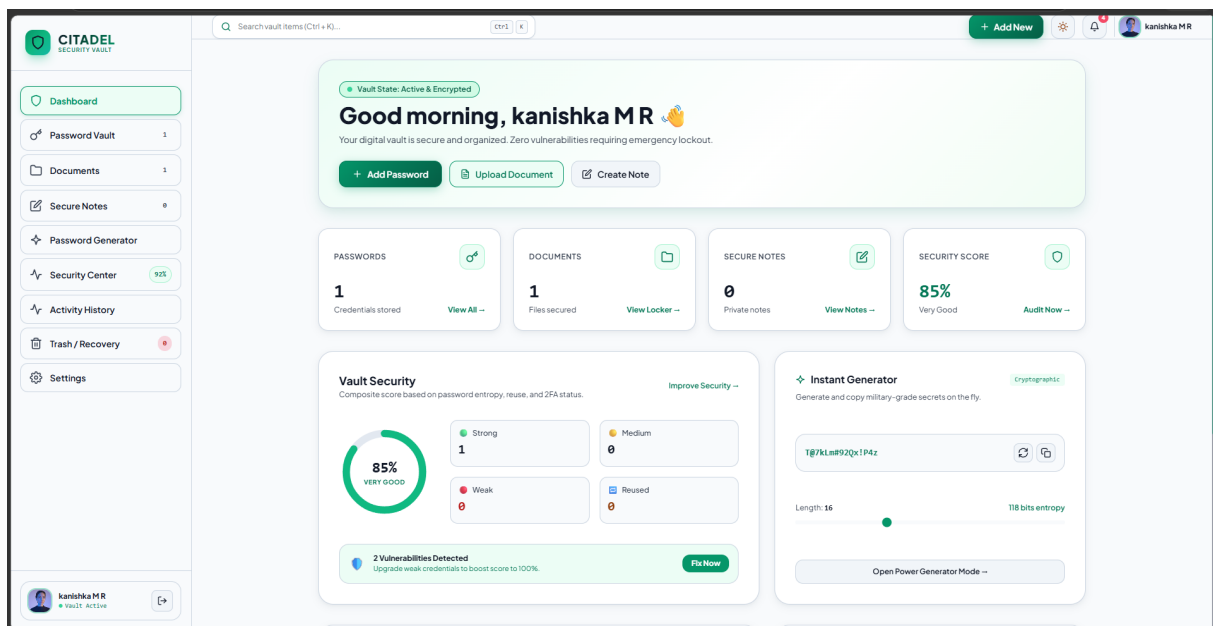


Figure 4. User dashboard.

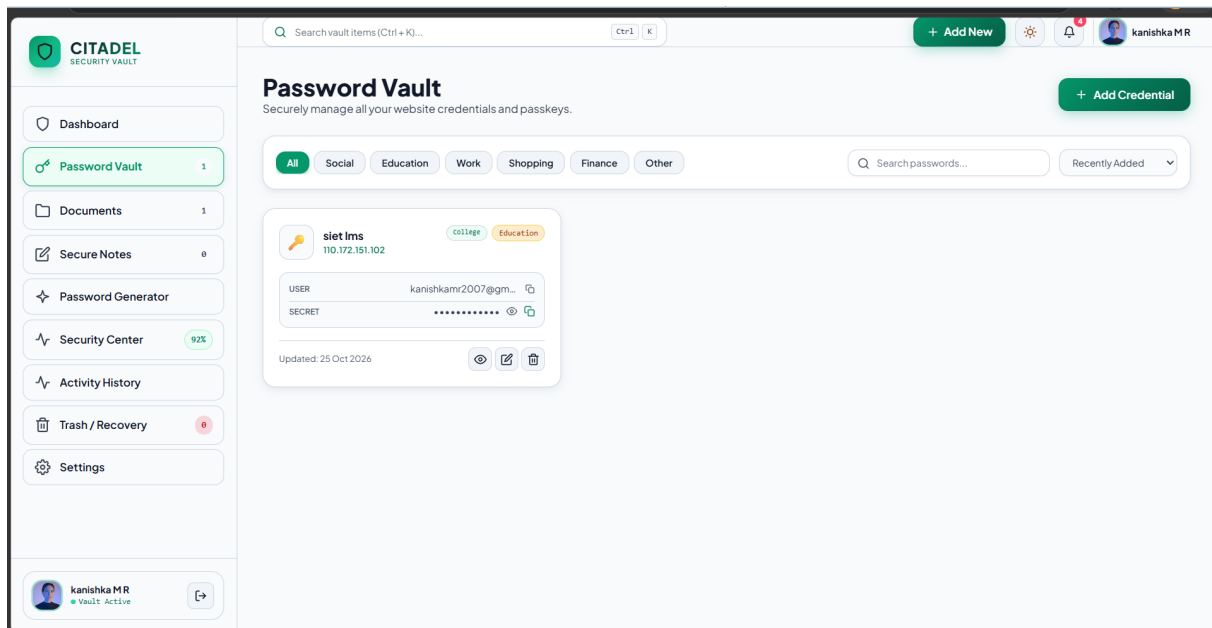


Figure 5. Password Vault module.

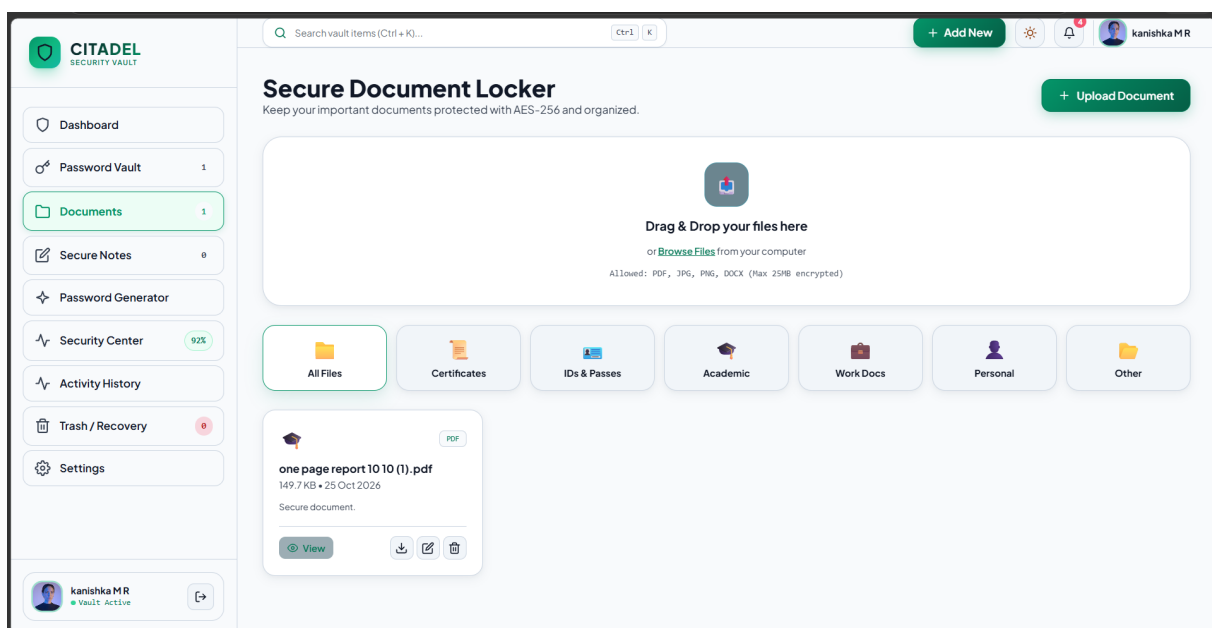


Figure 6. Secure Document Locker module.

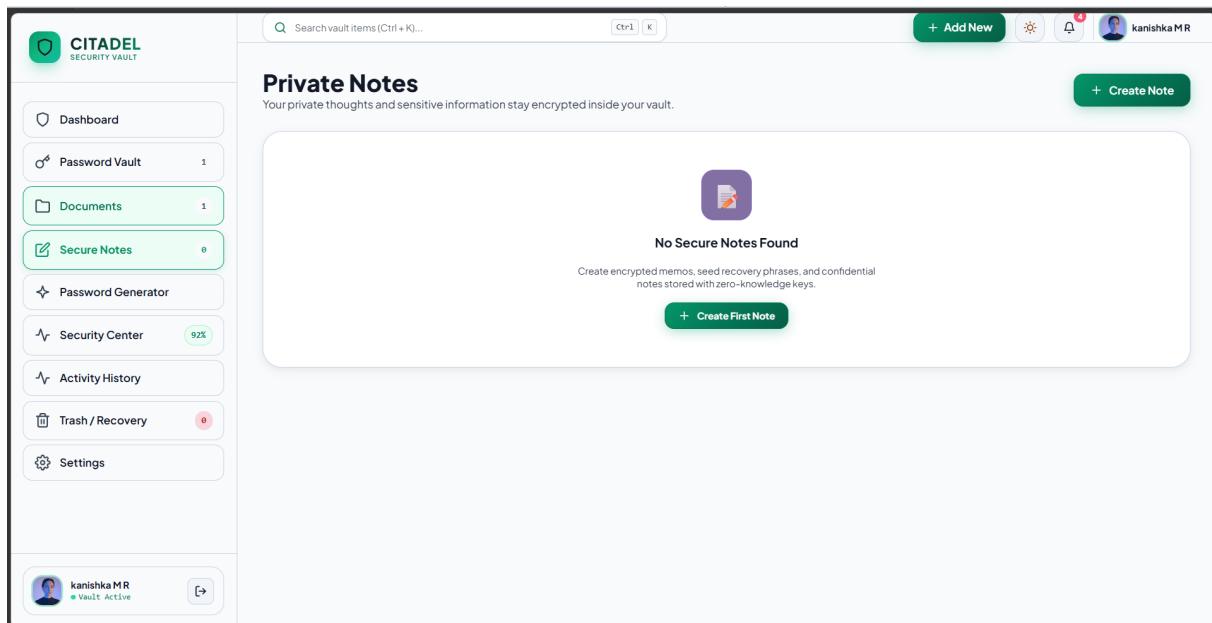


Figure 7. Private Notes module.

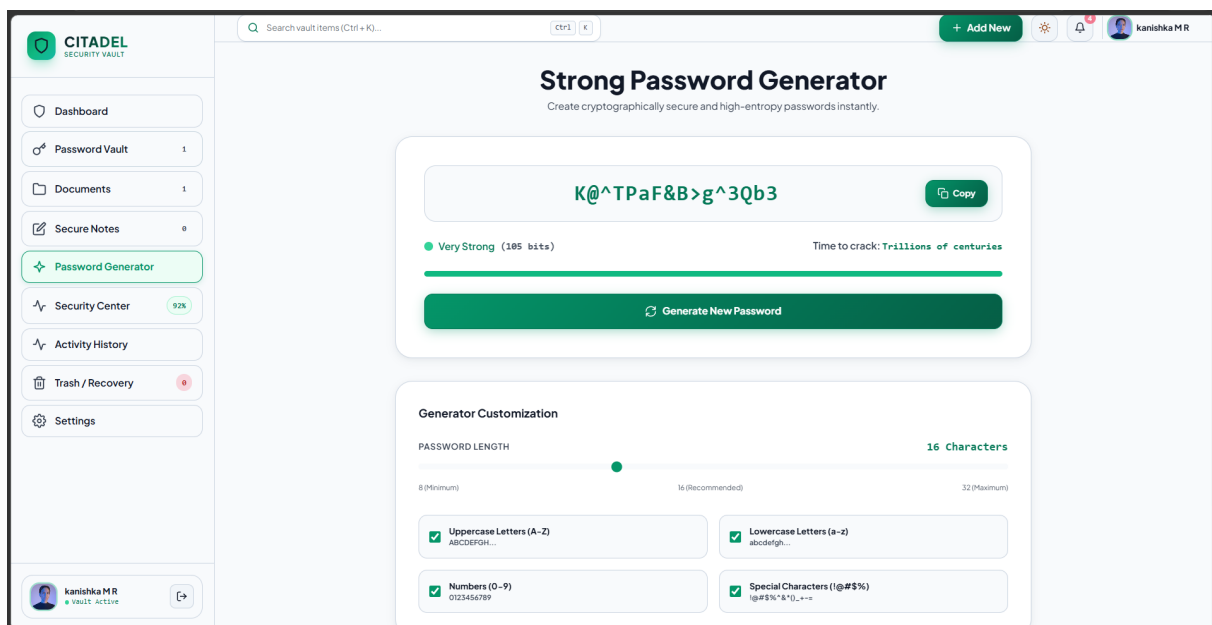


Figure 8. Password Generator module.

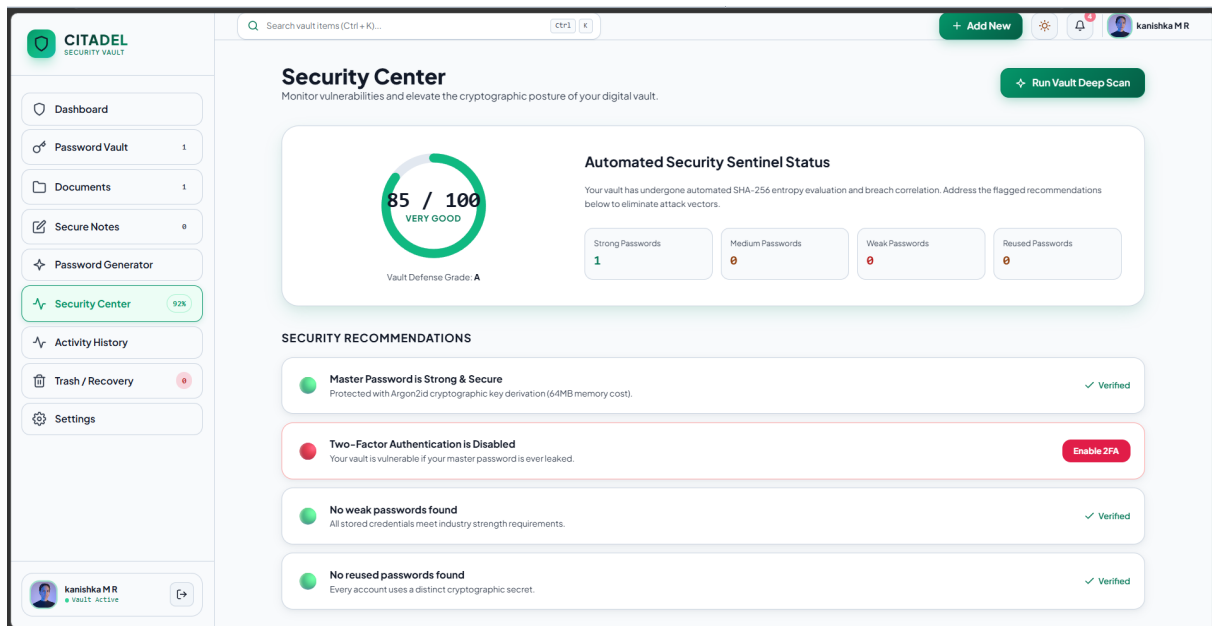


Figure 9. Security Center module.

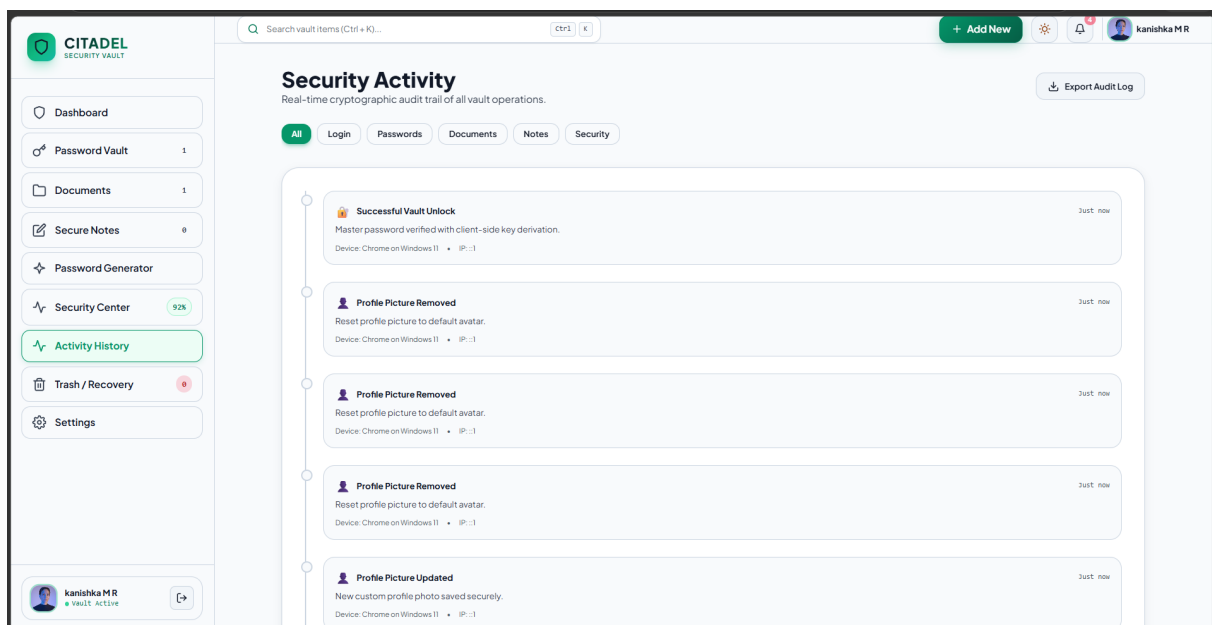


Figure 10. Activity History module.

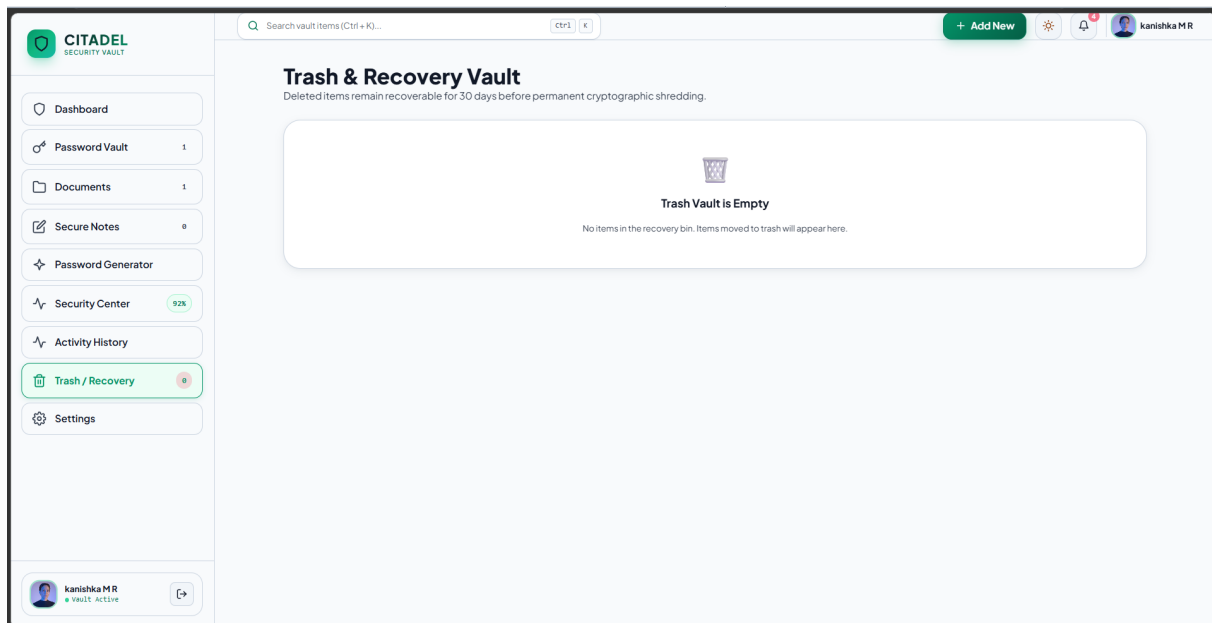


Figure 11. Trash and Recovery module.

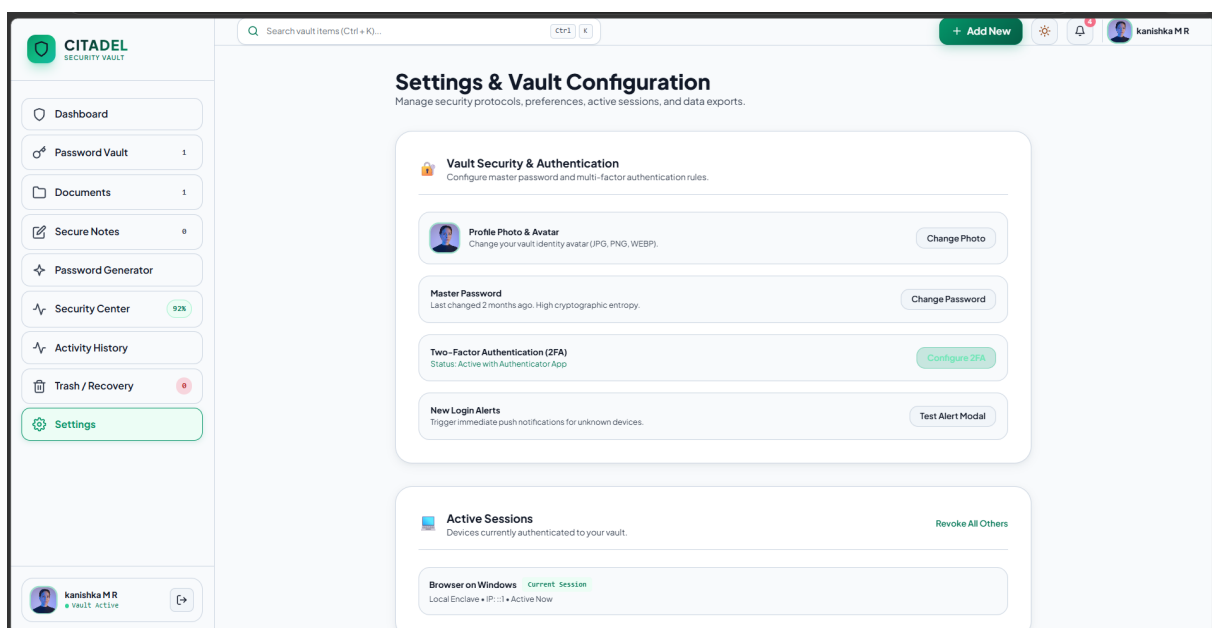


Figure 12. Settings and vault configuration page.

7 Conclusion

The CITADEL Security Vault provides a centralized platform for managing passwords, personal documents, private notes, and other confidential information. It aims to simplify digital information management by combining essential features in a single application.

The system allows users to organize login credentials for different websites and manage multiple accounts belonging to the same application separately. Features such as document storage, private notes, and password generation help users manage their personal information conveniently.

By integrating the frontend, backend, and database, CITADEL supports efficient information storage and retrieval. Appropriate authentication and encryption mechanisms help protect sensitive information and reduce the risk of unauthorized access.

Overall, CITADEL offers a convenient approach to personal digital information management. Future improvements can introduce additional security features, enhanced backup options, and advanced monitoring capabilities to improve the system's reliability and protection.

8 Future work

The CITADEL Security Vault can be enhanced in the future by integrating advanced security technologies and additional features. These improvements can strengthen data protection, improve accessibility, and provide a better user experience.

- **Multi-Factor Authentication:** Adding OTP or authenticator-based verification to provide an additional layer of security and prevent unauthorized access.
- **Advanced Encryption:** Improving encryption methods to protect passwords, private notes, and sensitive documents from unauthorized access.
- **Biometric Authentication:** Introducing fingerprint or facial authentication on supported devices for convenient and secure access.
- **Cloud Backup and Recovery:** Providing secure backups to help users restore their stored information if their device is lost or damaged.
- **Password Health Monitoring:** Identifying weak or reused passwords and providing recommendations to improve account security.
- **Security Notifications:** Sending alerts about suspicious login attempts and important changes to account settings.
- **Mobile Application:** Developing Android and iOS applications to allow users to access their vault through smartphones and tablets.
- **Browser Extension:** Integrating a browser extension to help users retrieve saved login credentials conveniently while browsing.
- **Improved Account Management:** Adding advanced labels and categories to organize multiple accounts belonging to the same application, such as personal, academic, and professional accounts.
- **Enhanced Document Management:** Introducing document expiry reminders, improved search options, and additional file organization features.
- **Activity Monitoring:** Maintaining a history of important actions, such as logins, password updates, and document uploads, to help users monitor vault activity.
- **Cloud Deployment:** Deploying the application on reliable cloud infrastructure to improve availability, scalability, and accessibility.

In the future, CITADEL can evolve into a comprehensive personal digital security platform by combining advanced authentication, secure storage, password monitoring, and cloud backup. These improvements can make the system more reliable, flexible, and convenient while helping users manage their digital information securely in one place.

References

- [1] OWASP Foundation. *Password storage cheat sheet*. OWASP Cheat Sheet Series; 2021.
- [2] Biryukov A, Dinu D, Khovratovich D. Argon2: New generation of memory-hard functions for password hashing and other applications. In: *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*. 2016. p. 292–302.
- [3] Grassi PA, Fenton JL, Newton EM, Perlner RA, Regenscheid AR, Burr WE, et al. Digital identity guidelines: Authentication and lifecycle management. NIST Special Publication 800-63B. Gaithersburg (MD): National Institute of Standards and Technology; 2017 (updated 2020).
- [4] Bonneau J, Herley C, van Oorschot PC, Stajano F. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In: *2012 IEEE Symposium on Security and Privacy*. 2012. p. 553–567.
- [5] Gaw S, Felten EW. Password management strategies for online accounts. In: *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS)*. 2006. p. 44–55.
- [6] Florêncio D, Herley C, van Oorschot PC. An administrator's guide to internet password research. *login: The USENIX Magazine*. 2014;39(4):35–41.
- [7] OWASP Foundation. *Cryptographic storage cheat sheet*. OWASP Cheat Sheet Series; 2021.
- [8] Dworkin M. Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC. NIST Special Publication 800-38D. Gaithersburg (MD): National Institute of Standards and Technology; 2007.
- [9] Rescorla E. *The Transport Layer Security (TLS) protocol version 1.3*. RFC 8446. Internet Engineering Task Force; 2018.
- [10] Fett D, Küsters R, Schmitz G. A comprehensive formal security analysis of OAuth 2.0. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 2016. p. 1204–1215.
- [11] MongoDB Inc. *MongoDB security and data protection*. MongoDB Technical Documentation; 2024.
- [12] OWASP Foundation. *Authentication cheat sheet*. OWASP Cheat Sheet Series; 2021.
- [13] OWASP Foundation. *File upload cheat sheet*. OWASP Cheat Sheet Series; 2021.
- [14] Herley C, van Oorschot PC. A research agenda acknowledging the persistence of passwords. *IEEE Security & Privacy*. 2012;10(1):28–36.
- [15] Mozilla Developer Network (MDN). *Web security*. MDN Web Docs.
- [16] van Oorschot PC, Salehi-Abari A, Thorpe J. Purely automated attacks on passpoints-style graphical passwords. *IEEE Transactions on Information Forensics and Security*. 2010;5(3):393–405.
- [17] Barker E. *Recommendation for key management: Part 1 – General*. NIST Special Publication 800-57 Part 1. Gaithersburg (MD): National Institute of Standards and Technology.