GuardFile Web Application Proposal:

GuardFile: Cloud-Based Secure File Storage System

By: Dylan Miller & Mina Astafanous

CPSC 490

Professor: Dr. Lidia Morrison

Department of Computer Science

California State University, Fullerton

Fall 2025

Table of Contents

Table of Figures

Abstract

The GuardFile system is a secure web based cloud application designed to help users safely store, organize, and manage personal files while maintaining the core cybersecurity principles of confidentiality, integrity, and availability. GuardFile applies strong security protections including asymmetric encryption, multi factor authentication, audit logs, malware scanning, and adaptive access control. Research in encryption and secure cloud storage shows that strong cryptographic methods are essential for protecting sensitive data in cloud environments (Al Saeed 2019; Vijayarangan and Florence 2023). To verify user identity, GuardFile integrates password authentication, face recognition, and voice matching, which aligns with modern research that highlights the importance of multi factor authentication for preventing unauthorized access (Zhou, Chekole, and Ang 2025).

GuardFile also provides real time email alerts and detailed audit logs that record sign in time, device, IP address, and general location to help users identify unusual activity. In addition to securing data, GuardFile features a Security Score system that educates users on safe digital practices and encourages stronger cybersecurity habits. By combining encryption, authentication, access control, and user education. GuardFile creates a practical and secure environment for individuals who want both protection and awareness while managing their data in the cloud.

1.0 Introduction

As digital storage becomes a major part of everyday life, users rely heavily on cloud services to manage important documents, photos, school assignments, and other personal files. Despite the convenience, many individuals remain unaware of how vulnerable their data can be without strong security measures. Cyberattacks, identity theft, man in the middle attacks, and weak authentication practices leave users exposed to dangerous threats. Research shows that cloud systems can be compromised when data is transmitted without strong cryptographic protection or when access control is mismanaged (Reece et al. 2024).

GuardFile was created to address these concerns by offering a secure and user-friendly cloud platform. It not only protects sensitive files through encryption and multi factor authentication but also informs users about safe cybersecurity practices. Instead of relying only on automated security features, GuardFile encourages users to understand and improve their protective habits. This combination of security and education supports long term digital safety.

1.1 Background

Many people assume their information is safe simply because it is stored in the cloud, but research shows that this is not always the case. Cloud environments are vulnerable to data leakage, insecure storage, weak keys, and unauthorized access when proper protections are not applied (Vijayarangan and Florence 2023). Users also frequently rely on password only authentication, which is no longer sufficient. Single factor authentication cannot reliably protect accounts, especially when passwords are weak or reused (Zhou et al. 2025).

Additionally, system design confidentiality is often overlooked. Sensitive information can be exposed during the development phase if proper modeling protections are not applied. Research on secure modeling shows that applying confidentiality rules and security policies early in the design process helps prevent unauthorized access to system details (Bourdellès, El Hachem, and Sadou 2024).

GuardFile responds to these challenges by using encryption, multi factor authentication, adaptive access control, malware scanning, and secure design principles. These methods ensure that user data remains protected at all stages, from login to storage.

1.2 Motivation

People store more digital information than ever before. Schoolwork, legal documents, personal photos, financial records, and identity information are frequently uploaded to cloud platforms. Unfortunately, many individuals do not understand how easily this information can be stolen, intercepted, or exposed if strong security measures are not in place. Research shows that encryption and access control are essential for protecting data stored in multi cloud systems (Reece et al. 2024). GuardFile is motivated by the need to give users a safe and simple way to protect their data without requiring deep technical knowledge.

Research also shows that multi factor authentication significantly reduces unauthorized access by adding additional layers of identity verification (Zhou et al. 2025). Combining knowledge factors with biometrics helps ensure that only verified users can access sensitive files. GuardFile implements these protections along with educational tools to encourage users to build safe habits.

Another motivation behind GuardFile is that many users are not aware of how to protect themselves from attacks. A system that both protects and teaches users creates a stronger defense against cyber threats. GuardFile's Security Score helps users understand their vulnerabilities and learn how to stay safe online.

1.3 Related Work

1.3.1 Multi Factor Authentication and Identity Verification

Multi factor authentication plays a major role in preventing unauthorized account access. Zhou, Chekole, and Ang (2025) explain that single factor authentication is no longer effective against modern cyber threats. Their study identifies eight important criteria used to evaluate multi factor authentication protocols and emphasizes the need for using more than one verification method. This research supports GuardFile's use of three layered authentication which includes password entry, face recognition, and voice verification.

1.3.2 Cloud Storage Encryption and Data Protection

Encryption is an essential part of secure cloud storage. Al Saeed (2019) demonstrated how asymmetric encryption protects confidential information by using a pair of public and private keys. Their findings show how encryption ensures that data remains secure even if intercepted.

Vijayarangan and Florence (2023) introduced a secure cloud storage mechanism that uses encryption, data dispersion, and distributed storage to prevent data leaks. They highlight how encryption protects files during transmission and at rest, which aligns with GuardFile's design to keep data unreadable to unauthorized individuals.

Research on multi cloud attacks also shows that web applications can be targeted through man in the middle attacks if data is not encrypted properly during communication (Reece et al. 2024). GuardFile applies Transport Layer Security to prevent interception and ensure safe data exchange.

1.3.3 Access Control and Requirements Confidentiality

Modern cloud systems must ensure that users only have access to the data they are authorized to view. Fernandes and Martins (2024) propose an adaptive role based access control model that adjusts permissions based on context such as user location, device, and session behavior. This research supports GuardFile’s plan to offer flexible file permissions and safe account management tools.

Confidentiality in system design is also important. Bourdellès, El Hachem, and Sadou (2024) highlight methods for applying the Bell La Padula model to prevent unauthorized access to system information during the design process. These concepts guide GuardFile's development strategy by emphasizing confidentiality at every stage.

2.0 Problem Statement

As cloud storage usage increases, so do security risks. Many users do not understand how vulnerable their data can be when stored online without strong protections. Weak authentication, poor encryption, insecure communication channels, and improper access control can all lead to data breaches. Research shows that man in the middle attacks, cloud misconfigurations, and system design errors can expose sensitive information (Reece et al. 2024; Bourdellès et al. 2024).

Another problem is the lack of user education. Cloud platforms often provide storage but do not teach users how to recognize unsafe habits such as using weak passwords or ignoring suspicious activity. This leads to higher levels of risk and greater chances of data loss. GuardFile aims to address these problems by implementing strong technical protections and providing user-friendly educational tools.

3.0 Proposed Project and Significance

GuardFile is a cloud based web application designed to provide secure file storage by using encryption, multi factor authentication, adaptive access control, and detailed audit logging. The system prevents unauthorized access while helping users understand safe cybersecurity practices. What makes GuardFile significant is its combination of protection and education.

Encryption protects files during storage and transfer, which directly supports research on cloud confidentiality and secure communication (Al Saeed 2019; Vijayarangan and Florence 2023). Multi factor authentication follows modern recommendations for reducing account compromises (Zhou et al. 2025). GuardFile also incorporates secure access control strategies, including adaptive permissions and confidentiality modeling, as recommended by Fernandes and Martins (2024) and Bourdellès et al. (2024).

Additionally, GuardFile includes a Security Score that helps users measure their safety level and improve their habits over time. This creates a complete solution that protects data and builds long term awareness, making GuardFile both effective and educational.

4.0 Objectives (Step by Step Requirements and UX)

Overall Project Objective

The main objective of GuardFile is to create a secure and user friendly cloud system that protects user data while teaching safe cybersecurity practices. GuardFile must apply encryption, authentication, access control, malware scanning, and education features in a way that is simple and accessible to users.

4.1 UX Design and Functions

4.1.1 Getting Started with GuardFile

Users access GuardFile through a web browser. The homepage allows them to sign up or log in.

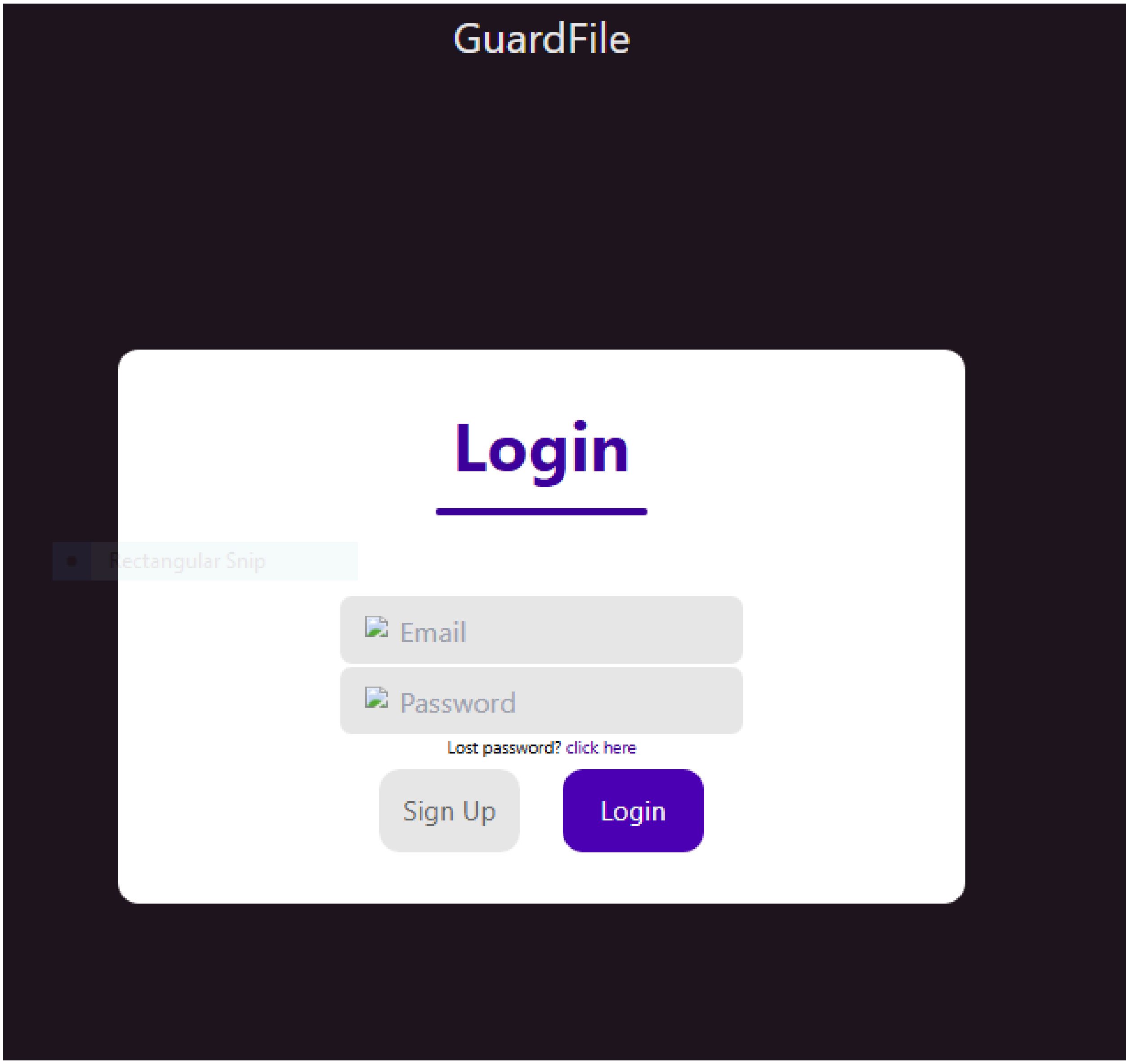


Figure 1 GuardFile Web Login Page

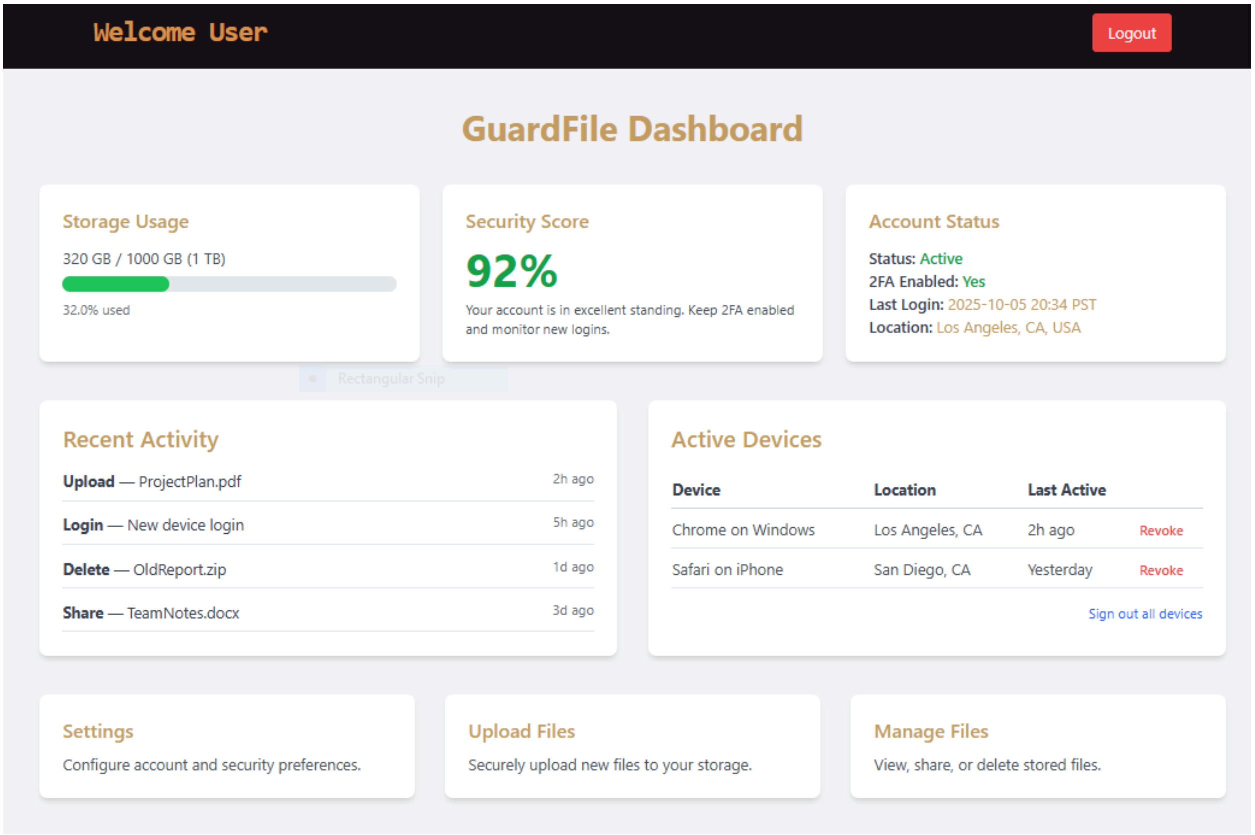
New users create an account by entering their first name, last name, and email address. Returning users sign in using their credentials and then complete multi factor authentication steps which include:

1. Password verification

2. Facial recognition using a device camera

3. Voice authentication through the user's microphone

These authentication methods follow strong security guidelines supported by MFA research (Zhou et al. 2025). After logging in, the user receives an email that includes sign in time, IP address, and location to help detect unusual activity. The user is then taken to the dashboard.



GuardFile Dashboard

Storage Usage

320 GB / 1000 GB (1 TB)

32.0% used

Security Score

92%

Your account is in excellent standing. Keep 2FA enabled and monitor new logins.

Account Status

Status: Active
2FA Enabled: Yes
Last Login: 2025-10-05 20:34 PST
Location: Los Angeles, CA, USA

Recent Activity

Upload — ProjectPlan.pdf	2h ago
Login — New device login	5h ago
Delete — OldReport.zip	1d ago
Share — TeamNotes.docx	3d ago

Active Devices

Device	Location	Last Active	
Chrome on Windows	Los Angeles, CA	2h ago	Revoke
Safari on iPhone	San Diego, CA	Yesterday	Revoke

Sign out all devices

Settings

Configure account and security preferences.

Upload Files

Securely upload new files to your storage.

Manage Files

View, share, or delete stored files.

Figure 2 GuardFile Dashboard

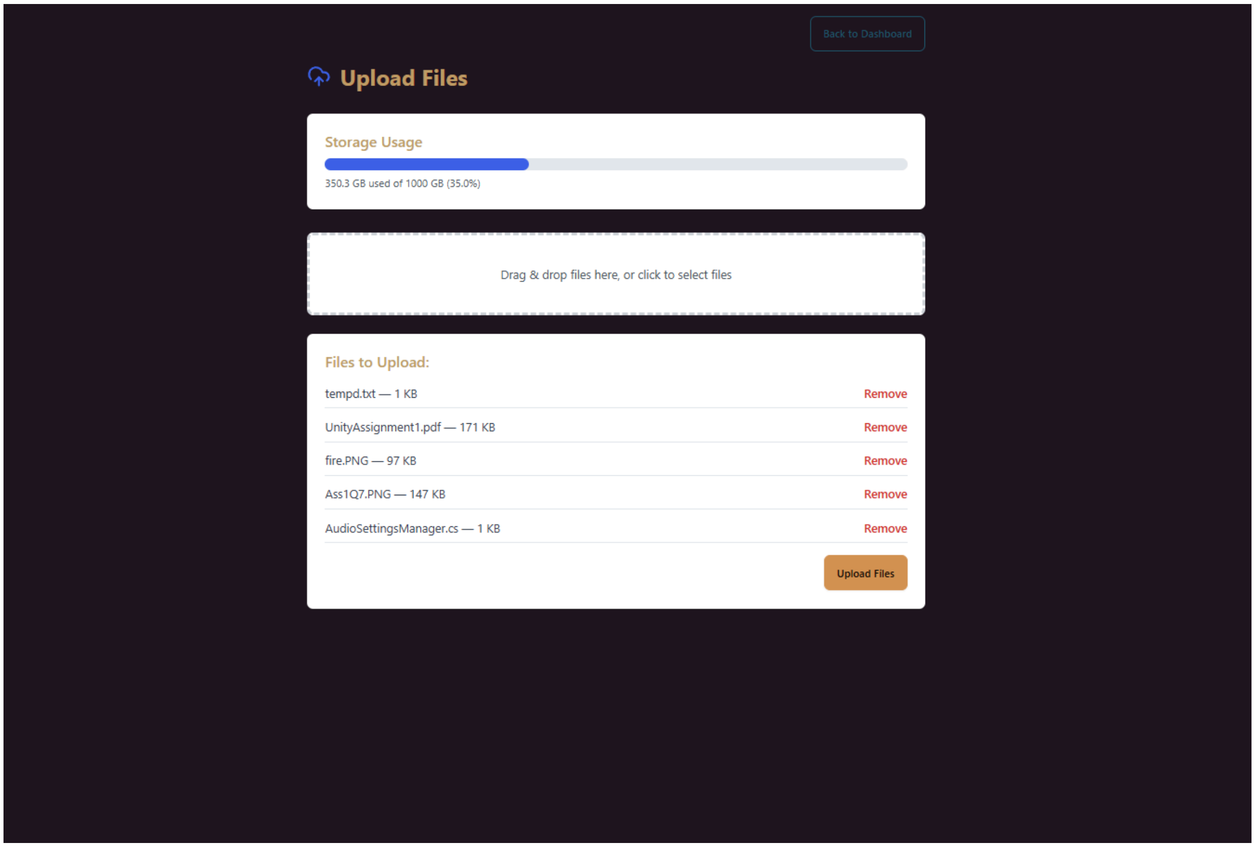
4.1.2 Creating the User Security Profile

During onboarding, users register their face data and voice sample. This information strengthens account protection by combining multiple identity factors. Users are also introduced to the Security Score system, which evaluates their account safety level. The system may suggest improvements such as updating passwords, enabling file level protection, or reviewing login history.

These recommendations are based on modern research in access control and user behavior adaptation (Fernandes and Martins 2024).

4.1.3 Uploading and Managing Files

Users upload files through the Upload Files section.



Upload Files

Storage Usage

350.3 GB used of 1000 GB (35.0%)

Drag & drop files here, or click to select files

Files to Upload:

tempd.txt — 1 KB

UnityAssignment1.pdf — 171 KB

fire.PNG — 97 KB

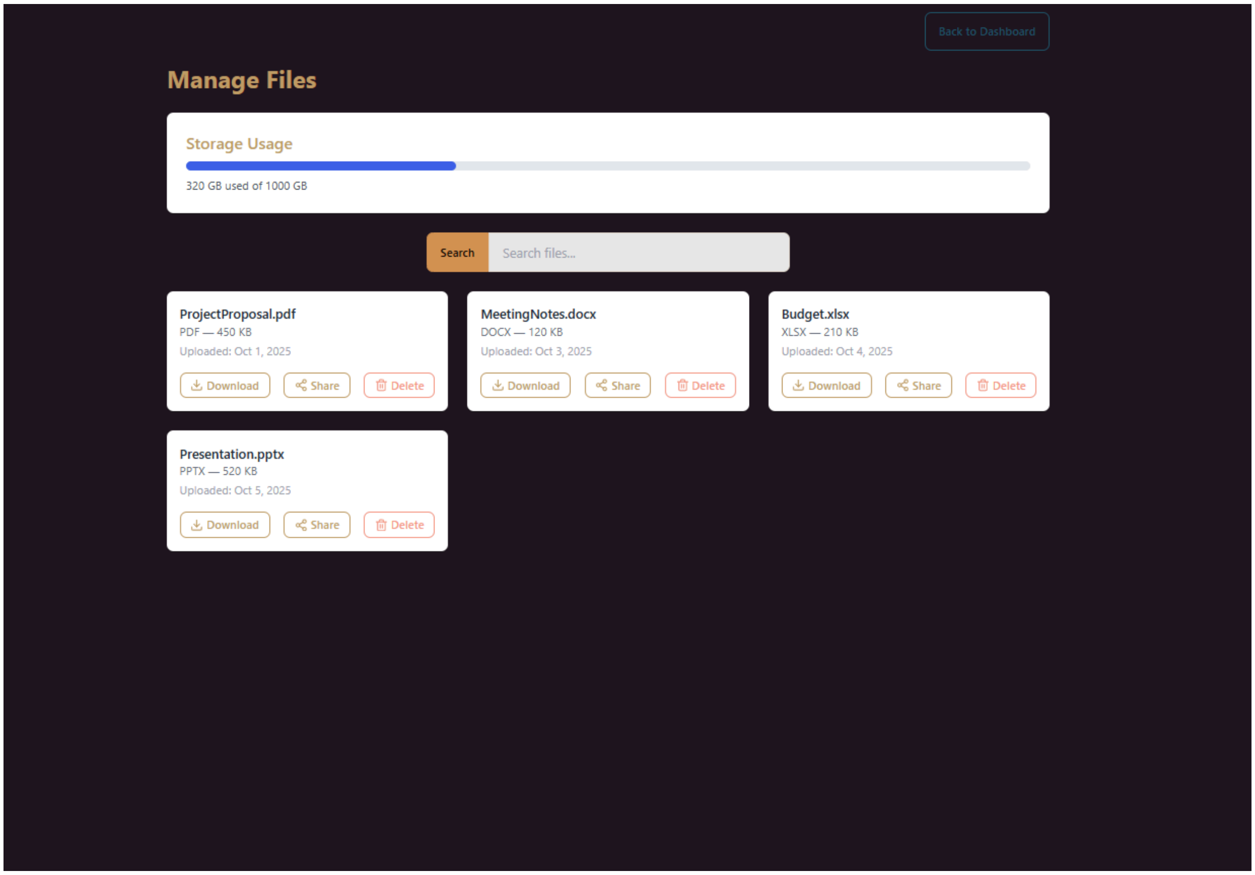
Ass1Q7.PNG — 147 KB

AudioSettingsManager.cs — 1 KB

Figure 3 GuardFile File Upload Page

Files can be added using the browse button or by dragging and dropping them into the upload area. Users may rename files before uploading and add optional password protection to sensitive files. Progress bars show upload status, and the system sends an email after each completed upload.

Users then manage files through the Manage Files page.



Manage Files

Storage Usage

320 GB used of 1000 GB

ProjectProposal.pdf
PDF — 450 KB
Uploaded: Oct 1, 2025

MeetingNotes.docx
DOCX — 120 KB
Uploaded: Oct 3, 2025

Budget.xlsx
XLSX — 210 KB
Uploaded: Oct 4, 2025

Presentation.pptx
PPTX — 520 KB
Uploaded: Oct 5, 2025

Figure 4 GuardFile File Management Interface

All files appear in a grid layout. Each file shows metadata including upload date and file size.

Users may:

- Search for files
- Download files

- Delete files

- Rename files

- Change file permissions

- View detailed information

Before downloading, all files are scanned for malware. This feature follows research on preventing man in the middle attacks and ensuring safe communication across cloud environments (Reece et al. 2024).

5.0 Activities

5.1 Functionality

GuardFile must support user registration, secure login, multi factor authentication, file upload, file management, permissions control, audit logging, and secure logout. All functions must operate smoothly and protect data consistency.

5.2 User Friendly Interface

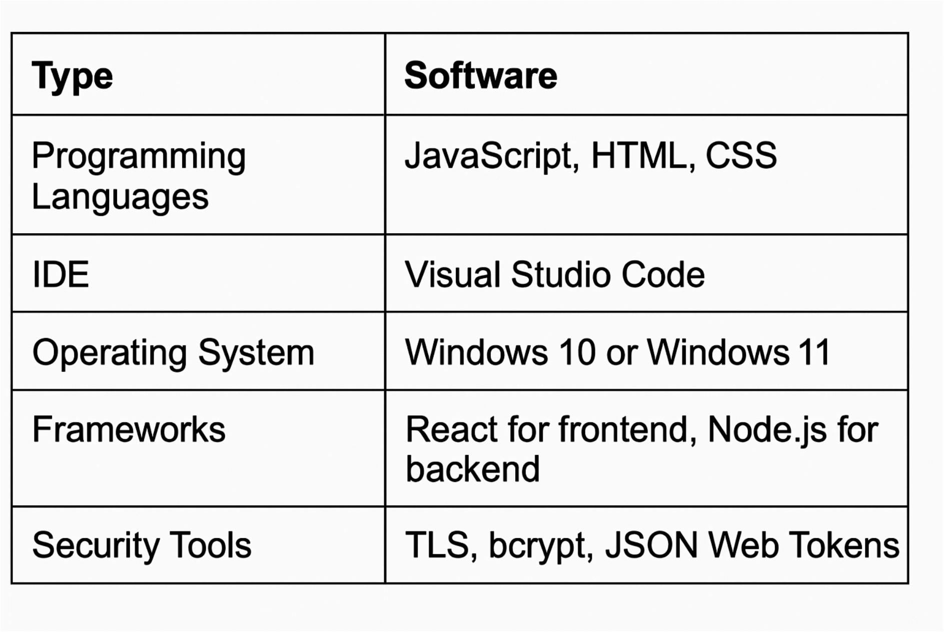
The design must be clean, organized, and easy to understand. A clear interface makes the platform more accessible, especially for users who are not familiar with cybersecurity. Testing will be done to collect feedback and improve usability.

5.3 Security

Security is the most important part of GuardFile. The system must apply encryption in transit and at rest, follow secure communication standards, protect confidentiality during the design and development process, and enforce strict access control based on user roles and context. These ideas directly follow established research in encryption, cloud security, and modeling confidentiality (Al Saeed 2019; Vijayarangan and Florence 2023; Bourdellès et al. 2024; Fernandes and Martins 2024).

6.0 Development Environment

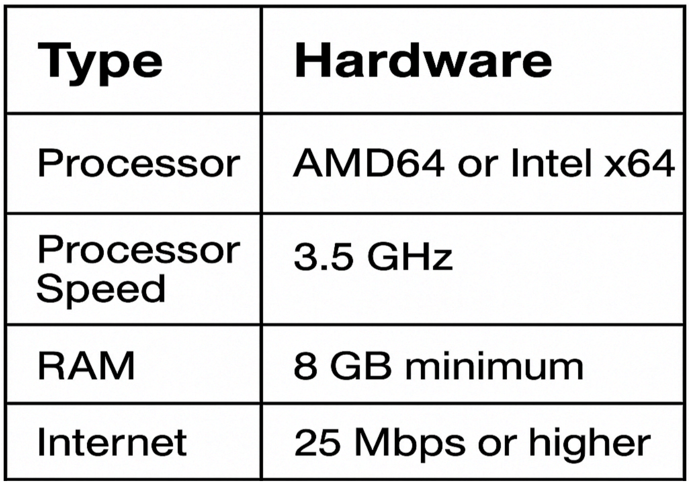
6.1 *Software Requirements*



Type	Software
Programming Languages	JavaScript, HTML, CSS
IDE	Visual Studio Code
Operating System	Windows 10 or Windows 11
Frameworks	React for frontend, Node.js for backend
Security Tools	TLS, bcrypt, JSON Web Tokens

Table 1: Software Requirements for GuardFile Web Application

6.2 Hardware Requirements



Type	Hardware
Processor	AMD64 or Intel x64
Processor Speed	3.5 GHz
RAM	8 GB minimum
Internet	25 Mbps or higher

Table 2: Hardware Requirements for GuardFile Web Application

7.0 Reports and Products

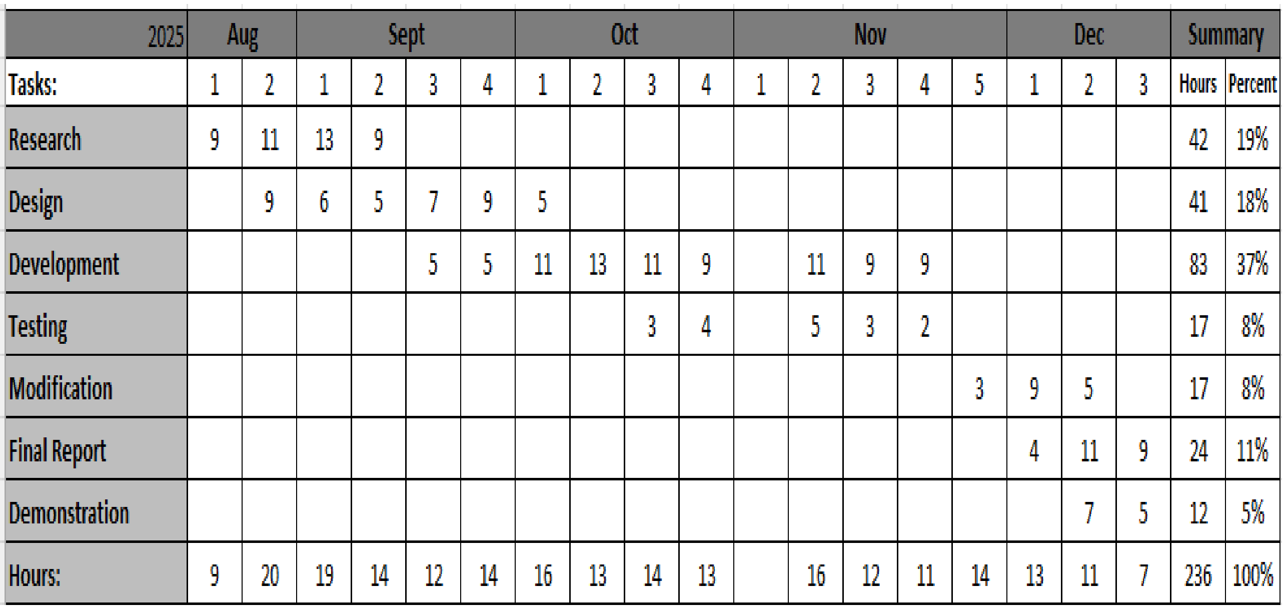
The final deliverables include:

- Cloud based web application
- Source code for frontend and backend
- UML diagrams
- System architecture diagram
- Audit log examples
- Testing documentation
- Step by step user guide
- Final report
- End of semester presentation

These materials will be evaluated by the project advisor and the Computer Science Department

8.0 Schedule

Below is the planned schedule for completion of this project within the timeframe of the Fall 2025 semester at California State University, Fullerton.



2025	Aug		Sept				Oct				Nov					Dec			Summary	
Tasks:	1	2	1	2	3	4	1	2	3	4	1	2	3	4	5	1	2	3	Hours	Percent
Research	9	11	13	9															42	19%
Design		9	6	5	7	9	5												41	18%
Development					5	5	11	13	11	9		11	9	9					83	37%
Testing									3	4		5	3	2					17	8%
Modification															3	9	5		17	8%
Final Report																4	11	9	24	11%
Demonstration																	7	5	12	5%
Hours:	9	20	19	14	12	14	16	13	14	13		16	12	11	14	13	11	7	236	100%

9.0 References

Al Saeed, Imad. “Applying Asymmetric Encryption Algorithm Using Kryptos.” Journal of Computing Sciences in Colleges, vol. 34, no. 4, 2019, pp. 110–113.

Bourdellès, M. El Hachem, J., and Sadou, S. “Ensuring Requirements Confidentiality During System Design Modelling.” Proceedings of the 39th ACM SIGAPP Symposium on Applied Computing, 2024.

Fernandes, J., and Martins, C. “Adaptive Role Based Access Control for Cloud Applications Using Context Aware Policies.” Proceedings of the 39th ACM SIGAPP Symposium on Applied Computing, 2024.

Reece, M., Lander, T., Mittal, S., Rastogi, N., Dykstra, J., and Sampson, A. “Defending Multi Cloud Applications Against Man in the Middle Attacks.” Proceedings of the 29th ACM Symposium on Access Control Models and Technologies, 2024.

Vijayarangan, E. V., and Florence, S. M. “Cloud Secure Storage Mechanism Based on Data Dispersion and Encryption.” Proceedings of the 4th International Conference on Information Management and Machine Intelligence, 2023.

Zhou, Jianying, Eyasu Getahun Chekole, and Kok Wee Ang. “Unveiling the Covert Vulnerabilities in Multi Factor Authentication Protocols.” ACM Computing Surveys, vol. 57, no. 11, 2025, pp. 1–37.