

# Etude Bibliographique

## Chapitre I : Contexte et enjeux

- I-1 : Importance du partage de fichiers en milieu collaboratif

### Évolution des environnements de travail et d'apprentissage

Dans le contexte actuel les environnements de travail et d'apprentissage ont considérablement évolué. La digitalisation progressive des processus a profondément transformé la manière dont les équipes collaborent. Le partage de fichiers est devenu une composante fondamentale de cette nouvelle réalité professionnelle et éducative. Le besoin d'échanger des documents de manière fluide entre collaborateurs ou entre étudiants et enseignants s'est intensifié avec l'essor du travail flexible, des équipes distribuées et des formations hybrides. Cette transformation organisationnelle a créé un besoin constant pour des solutions de partage efficaces, sécurisées et accessibles.

### Impact sur la productivité collective

Le partage de fichiers en environnement collaboratif représente un levier majeur de productivité pour plusieurs raisons :

- **Centralisation des ressources** : La disponibilité des documents dans un emplacement unique évite la dispersion de l'information et réduit le temps consacré à la recherche documentaire. Les études montrent qu'un employé passe en moyenne 1,8 heure par jour (soit 9,3 heures par semaine) à chercher des informations.
- **Travail simultané** : Les plateformes modernes permettent à plusieurs utilisateurs de travailler sur un même document, éliminant les problèmes de versions multiples et de conflits de modifications. Cette fonctionnalité peut améliorer l'efficacité des équipes jusqu'à 35% selon certaines études.
- **Continuité du travail** : L'accès aux fichiers depuis différents appareils et lieux garantit une continuité dans le flux de travail, particulièrement importante dans les contextes de travail hybride ou entièrement à distance.
- **Réduction des délais de communication** : Le partage instantané réduit considérablement les temps d'attente entre les différentes étapes d'un projet, accélérant ainsi les cycles de développement et de prise de décision.

## **Enjeux spécifiques aux milieux éducatifs**

Dans le cadre académique, comme celui de l'INPT mentionné dans le cahier des charges, le partage de fichiers présente des enjeux particuliers :

- **Distribution efficace des supports pédagogiques** : Les enseignants peuvent partager instantanément cours, exercices et ressources complémentaires avec tous les étudiants simultanément.
- **Remise et évaluation des travaux** : La centralisation des remises de travaux facilite leur suivi, leur évaluation et leur archivage pour les enseignants.
- **Apprentissage collaboratif** : Les étudiants peuvent travailler ensemble sur des projets communs, partageant ressources et résultats intermédiaires, favorisant ainsi l'intelligence collective.
- **Continuité pédagogique** : En cas d'impossibilité de présence physique, l'accès distant aux ressources garantit la poursuite des apprentissages.

## **Transformation des méthodes de travail en équipe**

Les solutions de partage de fichiers ont fondamentalement transformé les méthodes de travail **collectif** :

**Passage d'un modèle séquentiel à un modèle parallèle** : Auparavant, les documents circulaient d'un collaborateur à l'autre dans un processus linéaire. Aujourd'hui, plusieurs intervenants peuvent contribuer simultanément.

- **Démocratisation de l'accès à l'information** : Les hiérarchies informationnelles s'aplatissent au profit d'un accès plus égalitaire aux ressources, sous réserve des permissions appropriées.
- **Intégration dans des flux de travail complexes** : Le partage de fichiers s'intègre désormais dans des écosystèmes numériques plus larges (messageries, agendas partagés, outils de gestion de projet), créant une expérience de collaboration unifiée.
- **Facilitation du travail interdisciplinaire** : Les équipes transversales peuvent plus facilement combiner leurs expertises en accédant aux mêmes ressources.

## **Adaptation aux nouvelles réalités organisationnelles**

Les solutions comme L-Cloud répondent à des transformations organisationnelles profondes :

- **Organisations géographiquement dispersées** : Les équipes réparties sur plusieurs sites ou pays peuvent collaborer efficacement malgré la distance.

- **Flexibilité des horaires de travail :** Les collaborateurs peuvent accéder aux ressources selon leurs propres horaires, facilitant l'équilibre vie professionnelle vie personnelle.
- **Collaboration externe :** Le partage sécurisé avec des partenaires, clients ou consultants externes devient possible sans compromettre la sécurité globale du système.
- **Réduction de l'empreinte écologique :** La diminution significative de l'impression papier et des déplacements contribue aux objectifs de développement durable des organisations.

### **Défis spécifiques exigeant des solutions adaptées**

Cette importance croissante du partage de fichiers s'accompagne de défis que notre solution L-Cloud cherche à résoudre :

- **Équilibre entre accessibilité et sécurité :** Faciliter l'accès tout en protégeant les données sensibles.
- **Simplicité d'utilisation vs richesse fonctionnelle :** Proposer une interface intuitive sans sacrifier les fonctionnalités essentielles.
- **Gestion des droits différenciés :** Permettre un contrôle granulaire des accès tout en maintenant une administration simple du système.
- **Adaptation aux infrastructures existantes :** S'intégrer aux écosystèmes technologiques déjà en place dans les organisations.

En conclusion, le partage de fichiers n'est plus un simple outil technique mais un élément stratégique qui structure les modes de collaboration modernes. Notre projet LCloud s'inscrit dans cette évolution en proposant une réponse adaptée aux besoins spécifiques des environnements académiques et professionnels contemporains.

## **I-2 : Enjeux de la sécurité dans ces environnements**

### **Importance de l'aspect sécurité dans les environnements de partage collaboratif**

#### **La sécurité comme pilier fondamental du partage de fichiers**

Dans un contexte où la collaboration numérique s'intensifie, la sécurité des données partagées est devenue un enjeu critique. Cette dimension ne représente plus une simple option mais constitue l'ossature même sur laquelle repose la viabilité des plateformes collaboratives. La confiance des utilisateurs et l'intégrité des informations échangées dépendent directement du niveau de protection mis en œuvre.

## **Protection des actifs informationnels stratégiques**

Les documents partagés au sein des organisations ou des établissements d'enseignement représentent souvent un capital informationnel de haute valeur :

- **Données confidentielles et sensibles** : Documents administratifs, informations personnelles des utilisateurs, travaux de recherche non publiés, ou contenus pédagogiques propriétaires.
- **Propriété intellectuelle** : Dans le cadre académique comme l'INPT, les travaux de recherche, les innovations techniques et les productions étudiantes constituent un **patrimoine intellectuel à protéger**.
- **Informations stratégiques** : Plans de développement, documents contractuels ou données d'analyse qui, s'ils étaient compromis, pourraient avoir des conséquences significatives.

Une brèche de sécurité touchant ces actifs peut entraîner des conséquences graves : perte de compétitivité, atteinte à la réputation, complications juridiques ou perturbation des activités académiques.

## **Exigences réglementaires et conformité juridique**

Le cadre légal entourant la protection des données impose des obligations strictes aux gestionnaires de plateformes collaboratives :

- **Protection des données personnelles** : La loi marocaine 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et la loi 05-20 relative à la cybersécurité imposent des mesures spécifiques pour sécuriser les informations personnelles et les systèmes d'information.
- **Secteurs réglementés** : Certains domaines (santé, finance, défense) sont soumis à des contraintes supplémentaires concernant le stockage et le partage d'informations au Maroc.
- **Obligations contractuelles** : Les engagements pris auprès des utilisateurs ou des partenaires peuvent imposer des niveaux de sécurité définis.

La non-conformité à ces exigences expose l'institution à des sanctions administratives, financières et pénales, sans compter l'impact sur sa crédibilité.

## **La disponibilité : dimension cruciale de la sécurité**

Au-delà de la confidentialité et de l'intégrité, la disponibilité constitue un aspect fondamental de la sécurité dans les environnements collaboratifs :

- **Continuité de service** : L'accès ininterrompu aux ressources partagées est essentiel pour maintenir les flux de travail et respecter les échéances.
- **Résilience face aux incidents** : La capacité du système à résister aux défaillances techniques, aux pics d'utilisation ou aux tentatives de déni de service détermine sa fiabilité globale.
- **Accès multiplateforme** : Garantir la disponibilité depuis différents appareils et systèmes d'exploitation renforce l'utilité de la plateforme dans des contextes variés.
- **Performance sous charge** : Maintenir des temps de réponse acceptables même lors d'utilisations intensives préserve l'expérience utilisateur et la productivité.

Dans un contexte académique comme celui de l'INPT, où les périodes d'examens ou de remises de projets peuvent générer des pics d'utilisation, cette dimension revêt une importance particulière.

## **Menaces spécifiques aux environnements collaboratifs**

Les plateformes de partage font face à des vulnérabilités particulières qui justifient une attention renforcée :

- **Surface d'attaque élargie** : La multiplicité des utilisateurs, des appareils et des lieux de connexion augmente les points d'entrée potentiels pour les attaquants.
- **Risques d'erreurs humaines** : Le partage inapproprié, les mauvaises configurations des permissions ou les mots de passe faibles représentent des risques significatifs souvent sous-estimés.
- **Attaques ciblées** : Les plateformes centralisées contenant de nombreuses informations sensibles deviennent des cibles privilégiées pour les acteurs malveillants (rançongiciels, exfiltration de données, espionnage industriel ou académique).
- **Compromission de comptes** : L'usurpation d'identité d'un utilisateur disposant de droits étendus peut compromettre l'ensemble du système de partage.

## Sécurité vs Utilisabilité : un équilibre délicat

L'un des défis majeurs des plateformes comme L-Cloud réside dans la recherche d'un équilibre optimal entre :

- **Fluidité d'utilisation** : Les contraintes de sécurité ne doivent pas entraver l'expérience utilisateur au point de décourager l'adoption de la plateforme.
- **Contrôles rigoureux** : Les mécanismes de protection doivent être suffisamment robustes pour garantir l'intégrité et la confidentialité des données.
- **Transparence des mesures** : Les utilisateurs doivent comprendre les protections en place sans être surchargés de détails techniques.

Cette équation complexe explique pourquoi de nombreuses solutions commerciales échouent soit par excès de sécurité créant des frictions d'usage, soit par simplicité excessive conduisant à des vulnérabilités.

Dimensions essentielles de la sécurité dans un contexte collaboratif Une approche complète de la sécurité pour une plateforme comme L-Cloud doit intégrer plusieurs dimensions :

- **Authentification robuste** : L'identification fiable des utilisateurs constitue la première ligne de défense, justifiant le recours à des solutions comme le hachage des mots de passe avec bcrypt mentionné dans notre cahier des charges.
- **Contrôle d'accès granulaire** : La capacité à définir précisément qui peut accéder à quoi (lecture seule, modification, suppression) permet de limiter l'exposition des données sensibles.
- **Chiffrement des données** : La protection des fichiers confidentiels par chiffrement garantit que même en cas d'accès non autorisé à l'infrastructure, les données restent illisibles.
- **Traçabilité des actions** : L'enregistrement systématique des activités (audit trail) permet de détecter les comportements suspects et de reconstituer la chronologie en cas d'incident.
- **Sécurisation des communications** : Le protocole HTTPS mentionné dans nos spécifications assure la confidentialité des échanges entre les utilisateurs et la plateforme.

## Répercussions d'une sécurité défaillante

Les conséquences d'une sécurité inadéquate ne se limitent pas aux risques techniques :

- **Perte de confiance des utilisateurs** : Une violation de données peut durablement entacher la réputation de la plateforme et de l'institution qui l'héberge.

- **Interruption de service** : Les incidents de sécurité conduisent souvent à des indisponibilités prolongées, perturbant les activités qui dépendent de l'accès aux ressources partagées.
- **Coûts de remédiation** : Le temps et les ressources nécessaires pour restaurer un système compromis dépassent largement les investissements qu'aurait nécessités une sécurité préventive adéquate.
- **Impact psychologique** : La violation de la confidentialité peut avoir des répercussions significatives sur le sentiment de sécurité et le bien-être des utilisateurs concernés.

## La sécurité comme avantage différenciant

Dans le contexte de notre projet L-Cloud, l'approche sécuritaire ne doit pas être perçue uniquement comme une contrainte technique, mais comme un véritable argument différenciant :

- **Adaptation au contexte local** : En développant une solution spécifique, nous pouvons intégrer des considérations de sécurité particulièrement pertinentes pour **notre environnement académique**.
- **Transparence du fonctionnement** : Contrairement aux solutions commerciales "boîtes noires", notre plateforme peut offrir une visibilité complète sur les mécanismes de protection mis en œuvre.
- **Évolution maîtrisée** : La capacité à faire évoluer nos mesures de sécurité en fonction des retours utilisateurs et des nouvelles menaces constitue un atout considérable.

En conclusion, la sécurité représente bien plus qu'une simple couche technique dans un environnement de partage collaboratif – elle en constitue la condition même d'existence. Notre projet L-Cloud, en plaçant cette dimension au cœur de sa conception, répond à un enjeu fondamental des écosystèmes numériques contemporains.

- I-3 : fiche de projet + prototype :

### Fiche de projet :

#### Annexe 1 - Analyse des opportunités

Options	Avantages	Désavantages	Coûts
Developpement en interne	Bonne organisation	Restriction de l'environnement de travail	600 \$
acquisition d'une solution clés en main	Avancement rapide du projet	Contrainte créative	1,000 \$
Develloppement en externe	L'acquisition d'une bonne expertise	Exposition de données confidentielles à un agent extérieur	1,500 \$

#### Choix et justifications

### 3. Commentaires d'approbation:

Projet approuvé sous réserve de suivi rigoureux des contraintes techniques et de sécurité

Est-ce que le projet est en ligne avec les objectifs stratégiques de l'organisation:	<input checked="" type="checkbox"/>	NON	
Si oui, à quelle(s) stratégie(s) le projet se rattaché-t-il?	Organisation des meetings réguliers pour la répartition des taches		

### Analyse préliminaire

	Effort externe	Ressources matérielles et financières	Budget estimé
	Taux		
	5,000 MAD		
PROJET	0 MAD	1,000 MAD	20,000 MAD
Contingence d'estimation (%) :	40%	0 MAD	2,000 MAD
Total:	<b>0 MAD</b>	<b>1,000 MAD</b>	<b>22,000 MAD</b>

### Contraintes

### Hypothèses critiques

- \_Utilisation de technologies spécifiques (Python/Flask ou Node.js/Express, SQLite).
- \_Limitation à un environnement local pour les tests.
- \_Sécurité basique (hashage des mots de passe, HTTPS si applicable).
- \_Dépassement de budget.
- \_Annulation de l'encadrement
- \_Dissolution de l'équipe

### 2. Pertinence du projet

#### Avantages

#### Désavantages

- \_Service centralisé localement: gestion facile de sécurité.
- \_Clientèle prédictive minimale.
- \_Risque de perte significatif; système local.
- \_Capacité prédictive limitée.

### Les impacts de ne pas faire le projet (s'il y a lieu)

- \_Des failles de sécurité.
- \_Un manque d'organisation de partage des données.

## Description du projet

L'objectif principal de ce projet est de développer une plateforme sécurisée de partage de fichiers, permettant aux utilisateurs d'échanger des documents de manière fluide et protégée. Cette plateforme sera accessible via une interface web intuitive et garantira que seuls les utilisateurs autorisés pourront accéder aux fichiers partagés.

INCLUSION	EXCLUSION
<ul style="list-style-type: none"> <li>_Gestion des utilisateurs (création de comptes, authentification: l'utilisateur doit insérer ses identifiants qui lui ont été fournis par l'admin).</li> <li>_Partage de fichiers (téléchargement, téléversement et visualisation des fichiers partagés).</li> <li>_Sécurité de base (Confidentialité : Hashage des mots de passe, gestion des accès et permissions). Intégrité : Vérification des permissions, protection contre les modifications non autorisées. Disponibilité : Assurer l'accès aux fichiers et aux services en évitant les interruptions. Cela permet d'assurer que les trois aspects fondamentaux de la sécurité sont bien pris en compte dans ton projet.</li> <li>_Interfaces simples (un interface d'authentification et des interfaces d'utilisateurs et de l'admin ).</li> </ul>	<ul style="list-style-type: none"> <li>_Fonctionnalités avancées de collaboration (chat, commentaires).</li> <li>_Gestion des versions de fichiers.</li> <li>_Support pour des environnements de production complexes (cloud, haute disponibilité).</li> <li>_Mesures de Sécurité pas trop avancées</li> </ul>

## 1. Présentation du projet

Titre:	<i>Inauguration d'une plateforme d'échange de fichier en ligne</i>	No du projet:	5
Client:	Équipes d'administrateurs\chef d'administration	Type de projet:	Plateforme de Partage de fichiers
Région:	INPT	Programme:	Développement d'une solution de partage de fichiers sécurisée
Date de début proposée		Budget proposé	
Responsable de l'analyse:	Mme.Hanine\Mme.Ayache	Courriel	<a href="mailto:hanine@inpt.ac.ma">hanine@inpt.ac.ma</a> <a href="mailto:ayache@inpt.ac.ma">ayache@inpt.ac.ma</a>
Responsable client:	Anaddam Mohamed	Courriel	<a href="mailto:anaddam.mohamed@inpt.ac.ma">anaddam.mohamed@inpt.ac.ma</a>
Promoteur:	Akallal Mohamed Issam	Courriel	<a href="mailto:akallal.mohamedissam@inpt.ac.ma">akallal.mohamedissam@inpt.ac.ma</a>

## Contexte

Dans un environnement de travail en réseau local ou dans un cadre éducatif, le besoin de partager des fichiers entre utilisateurs est courant. Cependant, même dans des contextes simples, il est crucial de garantir que seuls les utilisateurs autorisés puissent accéder aux fichiers. Ce mini-projet vise à développer une plateforme de base pour faciliter le partage sécurisé de fichiers, tout en offrant des fonctionnalités simples de collaboration.

## Prototype + description :

The login page has a white background. At the top is a circular logo featuring a shield with a blue and white design. Below the logo is the text "Welcome again!" in bold black font. Underneath that is a smaller text "Please enter your details". There are two input fields: one for "Email" and one for "Password". To the right of the password field is a "Remember me" checkbox and a "Forgot Password?" link. Below the input fields are two buttons: a green "Log In" button and a grey "Log in with Email" button.

The user interface shows a top navigation bar with "log out →", "REPORT", "Contact us", and a user icon. The main title "CHOOSE YOUR MODE" is centered above three large buttons. The first button, "Browse", contains a globe icon and the text "Browse". The second button, "Upload", contains a cloud with an upward arrow icon and the text "Upload". The third button, "Admin", contains a gear with a person icon and the text "Admin".

log out →

REPORT

Contact us



## CHOOSE YOUR MODE

Browse



Upload



Back

## BROWSE

[Folder 1](#)

[Folder 2](#)

[Folder 3](#)

[Folder 4](#)

[Folder 5](#)

[Folder 6](#)

**Selected: Folder 3**

File 1

File 2

File 3

File 4

Back

## BROWSE

- [User1](#)
- [User 2](#)
- [User 3](#)
- [User 4](#)

**Selected: User 2**

Username:  
[User 1](#)

Password:  
[Ex@mplepassw0rd2024](#)

## Uploaded Files

- [Folder 1](#)
- [Folder 4](#)
- [File 3](#)
- [File 4](#)

## MY SPACE

search by username, file name, folders, groups..

- [groups](#)
- [profile](#)
- [settings](#)
- [support](#)
- [back](#)

## **COMMENTAIRES :**

Voici notre page de connexion, où nos utilisateurs peuvent se connecter avec leur adresse e-mail et leur mot de passe.

**Page 2/3 :** Tout d'abord, l'utilisateur peut se déconnecter, signaler un problème ou un bug, ou nous contacter pour toute aide dont il pourrait avoir besoin, grâce aux trois boutons situés en haut. De plus, lorsqu'il se connecte, il doit choisir s'il souhaite se connecter en tant qu'administrateur pour gérer son groupe, télécharger un fichier/dossier ou parcourir ceux existants.(page 2 est celle de l'admin tandis que la page 3 est celle d'un utilisateur normal).

**Page 4 :** Nous avons réservé un espace utilisateur où il peut gérer ses propres fichiers , profil , les réglages etc.

**Page 5 :** Au cas où un utilisateur a choisi 'Browse' pour parcourir les données, cette interface permettra de gérer les fichiers et dossiers et d'accéder aux dossiers sur la même page.

**Page 6 :** représente l'interface 'Browse' de l'admin où il peut accéder aux fichiers de tous les utilisateurs et les manipuler à sa guise

## **• I-4 : Présentation des solutions et plateformes existantes :**

### **Présentation des plateformes de partage de fichiers**

 Objectif : Étudier les solutions existantes de partage de fichiers dans un contexte collaboratif, en mettant l'accent sur les mécanismes de sécurité qu'elles intègrent.

- Importance des plateformes dans le télétravail, l'éducation, les entreprises
- Centralisation du stockage et accessibilité à distance
- Risques : interception, fuites, compromission d'identités
- Besoin de sécurité : confidentialité, intégrité, disponibilité

### **Google Drive – Solution de Google Workspace**

- Stockage cloud collaboratif intégré à Gmail, Docs, etc.
- Contrôle des permissions (lecture, édition, commentaire)
- Synchronisation multi-appareils

## Sécurité :

- Chiffrement AES-256 au repos / TLS en transit
- Authentification forte (2FA)
- Détection d'activités suspectes via IA Limites :
- Données hébergées aux États-Unis (enjeux de souveraineté)
- Pas de chiffrement de bout en bout natif

Limites :

- Données hébergées aux États-Unis (enjeux de souveraineté)
- Pas de chiffrement de bout en bout natif

## **Dropbox – Simplicité et efficacité**

- Interface simple, accessible pour les particuliers et entreprises
- Partage via liens sécurisés ou comptes utilisateurs
- Versionnage automatique des fichiers

## Sécurité :

- Chiffrement AES-256 / TLS
- Vérification en deux étapes
- Journaux d'activité pour les entreprises Limites :
- Pas de chiffrement de bout en bout intégré
- Intégration professionnelle moins poussée que Google ou Microsoft

## **OneDrive – Intégration Microsoft**

- Intégré à Microsoft 365 (Word, Excel, Teams...)
- Collaboration en temps réel sur les documents
- Gestion centralisée des accès

## Sécurité :

- Chiffrement au repos et en transit
- Protection des informations (IRM / DLP)
- Authentification multi-facteurs

Limites :

- Configuration parfois complexe
- Fortement dépendant de l'écosystème Microsoft Slide 5 : Nextcloud – Solution open-source auto-hébergée
- Plateforme libre, orientée souveraineté et contrôle des données
- Extensions : chat, calendrier, webmail, etc.
- Possibilité d'auto-hébergement

## Nextcloud – Solution open-source auto-hébergée

### Sécurité :

- Chiffrement en transit / chiffrement bout en bout optionnel
- Authentification à deux facteurs
- Journalisation et contrôle d'accès Limites :
- Maintenance technique requise
- Interface moins intuitive selon les configurations

## Tableau comparatif

Solution	Chiffrement	Collaboration	Auto-hébergement	Souveraineté	Sécurité Globale
Google Drive	AES-256 + TLS	Excellente	✗	Faible	Élevée
Dropbox	AES-256 + TLS	Bonne	✗	Faible	Moyenne
OneDrive	AES-256 + IRM + TLS	Excellente	✗	Faible	Très élevée
Nextcloud	E2EE (optionnel)	Bonne	✓	Forte	Variable

- I-5 : Analyse des technologies utilisées :

### Protocoles de communication

Dans sa version actuelle, l'application repose sur le framework Flask, qui utilise par défaut le protocole HTTP pour établir la communication entre le client (navigateur) et le serveur.

HTTP est un protocole simple et largement utilisé pour le transfert de données web, mais il ne chiffre pas les échanges. Cela signifie que les données échangées peuvent être interceptées si le réseau est compromis.

Ce choix est acceptable dans un environnement de développement local ou pour des usages limités en circuit fermé (LAN). Cependant, pour un usage en production ou sur un réseau exposé à Internet, il est fortement recommandé de basculer vers HTTPS, qui ajoute une couche de sécurité via le protocole TLS (Transport Layer Security).

### Mécanismes de chiffrement

Le chiffrement dans notre projet intervient principalement lors de la gestion des mots de passe utilisateurs.

Nous utilisons les fonctions `generate_password_hash()` et `check_password_hash()` fournies par le module `Werkzeug.security`, une bibliothèque reconnue dans l'écosystème Flask.

Ce système repose sur l'algorithme PBKDF2 (Password-Based Key Derivation Function 2), ou bcrypt selon les paramètres de configuration. Ces algorithmes sont conformes aux standards de sécurité actuels, car ils appliquent un salage (salt) et des milliers d'itérations pour rendre les attaques par force brute ou dictionnaire très complexes.

- Les mots de passe sont hachés avant d'être stockés en base de données.
- Aucune information sensible n'est conservée en clair.
- La vérification d'authenticité ne nécessite jamais d'exposer le mot de passe original, assurant ainsi la confidentialité et l'intégrité des données utilisateur.

### Authentification

L'application met en œuvre un système d'authentification classique basé sur un formulaire contenant le nom d'utilisateur et le mot de passe.

Lorsque les identifiants sont valides, Flask stocke les informations de session dans des cookies côté client via la variable `session[]`. Cela permet à l'application de :

- Maintenir l'état de connexion de l'utilisateur tout au long de sa navigation.
- Déterminer ses droits d'accès (utilisateur standard ou administrateur).
- Rediriger automatiquement vers le tableau de bord approprié selon le rôle.

De plus, un middleware global (@app.before\_request) est utilisé pour intercepter toutes les requêtes entrantes. Il vérifie que l'utilisateur est bien connecté avant d'autoriser l'accès aux routes sensibles.

En l'absence de session active, l'utilisateur est automatiquement redirigé vers la page de connexion, ce qui renforce la sécurité et l'isolement des pages protégées.

- I-6: Comparaison des solutions en fonction de leurs avantages et limites

### Protocoles et normes de sécurité

Protocole / Norme	Rôle	Utilisation / Intégration actuelle
<b>HTTP</b>	Protocole de communication non sécurisé	Utilisé par défaut pour les échanges client/serveur
<b>TLS (HTTPS)</b>	Chiffrement des échanges	✗ Non encore implémenté
<b>PBKDF2 / bcrypt</b>	Hachage sécurisé des mots de passe	✓ Implémenté via Werkzeug
<b>Sessions sécurisées Flask</b>	Suivi de session	✓ Présent mais améliorable (signature, durée)
<b>AES (Advanced Encryption Standard)</b>	Chiffrement des fichiers	✗ Non encore implémenté

## Comparaison avec des solutions existantes

Critères	Projet actuel	Google Drive	Dropbox
Hébergement	Local	Cloud Google	Cloud Dropbox
Authentification	Simple (login/password)	OAuth, 2FA	OAuth, 2FA
Chiffrement fichiers	✗ Non chiffrés	✓ Oui (au repos et en transit)	✓ Oui
Contrôle des accès	✓ Basé sur rôle	✓	✓
Confidentialité	✓ Totale (hébergement local)	✗ Dépend du fournisseur	✗ Dépend du fournisseur



