La sécurité est un aspect essentiel pour toute application, notamment pour garantir la confidentialité et l'intégrité des données utilisateur. Voici quelques éléments essentiels à inclure dans l’analyse des besoins en matière de sécurité :

1. **Utilisation du protocole HTTPS** : L'utilisation de HTTPS est essentielle pour protéger les données transitant entre l'application mobile et le serveur. Le protocole HTTPS utilise un cryptage SSL/TLS pour chiffrer les données, empêchant ainsi toute interception ou altération des données en transit.
2. **Vérification de l'identité** : On peut utiliser le serveur Odoo pour vérifier l'identité de l'utilisateur lorsqu'il se connecte à l'application. On peut également utiliser des mécanismes d'authentification tels que la vérification par clé API pour renforcer la sécurité de l'application. Une option existe sur Odoo qui permet à un utilisateur de générer une clé unique d’identification, cette clé unique ne peut servir que pour un seul utilisateur et sur une seule application tierce. (Clé api non implémentée dans l’application car non demandé).
3. **Gestion des fichiers** : iOS fournit un environnement sécurisé pour les applications, ce qui signifie que les fichiers créés par une application ne sont accessibles que par cette dernière. On peut utiliser cette fonctionnalité pour garantir que les données de l'application ne sont pas accessibles à d'autres applications ou à des utilisateurs non autorisés.
4. **Protection contre les attaques de force brute** : Les attaques de force brute sont des tentatives répétées pour deviner un mot de passe ou une clé d'accès. On peut inclure des mécanismes de protection tels que la mise en place de limites de connexion. (Non implémenté dans l’application car non demandé).

Il est important de s’assurer que l’application offre un niveau de sécurité suffisant pour protéger les données des utilisateurs et garantir la confidentialité et l’intégrité des données.