Réalisation d’une application de vote en ligne avec JAVA EE

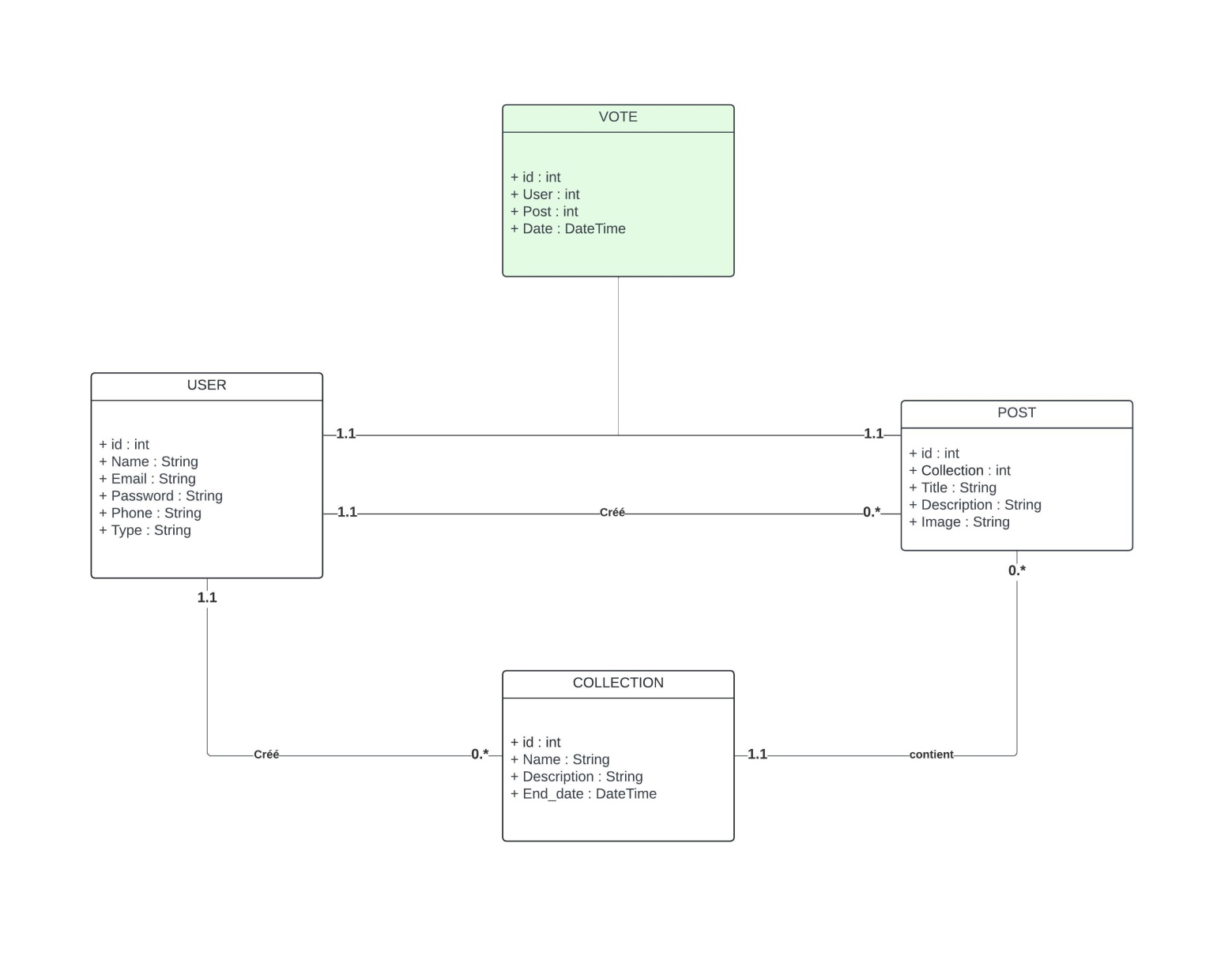
1. Concepts de sécurité appliqués :

* Authentication and Authorization.
* Chiffrement des Données:
  + Chiffrez les données sensibles au repos en utilisant des algorithmes de chiffrement forts comme AES par exemple j’ai utilisé l’algorithme AES pour chiffrer le mot passe.
* Communication Sécurisée :
  + Validez et assainissez toutes les données d'entrée pour prévenir les attaques par injection.
* Contrôle d'Accès :
  + Mettez un mécanismes de contrôle d'accès solides pour restreindre l'accès aux données et fonctions sensibles.

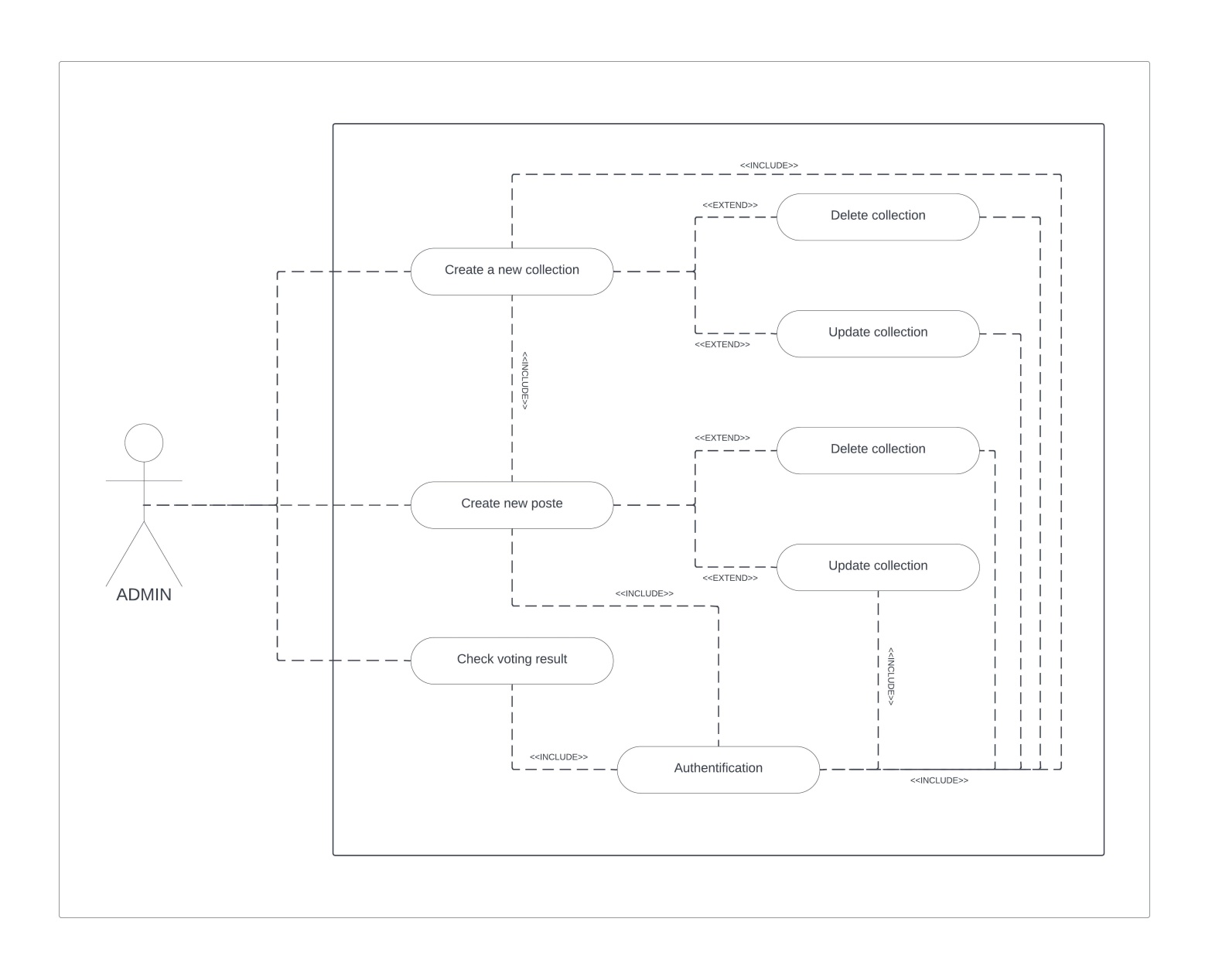
1. Vulnérabilités Courantes dans les Applications Distribuées :

* Injection SQL :
  + Se produit lorsque des instructions SQL malveillantes sont exécutées par l'application. Prévenez cela en utilisant des instructions préparées et des requêtes paramétrées.
* Cross-Site Scripting (XSS) :
  + Implique l'injection de scripts malveillants dans des pages web vues par d'autres utilisateurs. Atténuez cela en encodant correctement les sorties et en assainissant les entrées des utilisateurs.
* Cross-Site Request Forgery (CSRF) :
  + Trompe les utilisateurs pour qu'ils effectuent des actions qu'ils n'ont pas l'intention de faire en exploitant leurs sessions authentifiées. Utilisez des jetons anti-CSRF pour vous protéger contre cela.
* Désérialisation Insecure :
  + Peut entraîner une exécution de code à distance si des données non fiables sont désérialisées. Assurez-vous que les données sont validées et utilisez des bibliothèques de désérialisation sécurisées.
* Attaques Man-in-the-Middle (MITM) :
  + Interceptent et modifient les communications entre deux parties. Utilisez un chiffrement fort et des protocoles de communication sécurisés pour vous protéger contre cela.
* Authentification et Gestion des Sessions Brisées :
  + Peut entraîner un accès non autorisé si les jetons de session ne sont pas gérés de manière sécurisée. Utilisez de bonnes pratiques de gestion des sessions et un stockage sécurisé des jetons.
* Exposition des Données Sensibles :
  + Implique la fuite de données sensibles en raison d'un chiffrement ou de contrôles d'accès inadéquats. Assurez-vous que toutes les données sensibles sont chiffrées et que l'accès est restreint.
* Mauvaise Configuration de Sécurité :
  + Se produit lorsque les paramètres de sécurité sont mal configurés ou laissés par défaut. Révisez et mettez régulièrement à jour les configurations pour suivre les meilleures pratiques.

1. Conception :
2. Diagramme de classe :



1. Diagramme de cas d'utilisation <<Admin>>:



1. Diagramme de cas d'utilisation <<Client>> :

