جامعة مولاي إسماعيل
UNIVERSITÉ MOULAY ISMAÏL

كلية العلوم والتقنيات
FACULTÉ DES SCIENCES ET TECHNIQUES

Chiffrement basé sur les attributs: KP-ABE & CP-ABE

3ème année Cycle d'Ingénieurs en Génie Informatique

Module : Cryptographie et sécurité informatique

Réalisé par :
Bahida Anwar

Responsable : Prof Amounas Fatima

Plan

1 Introduction

Introduction

Contexte de la cryptographie moderne

Dans un monde où les données numériques circulent librement sur Internet, la confidentialité et le contrôle d'accès sont devenus des enjeux majeurs. Les schémas de chiffrement traditionnels ne permettent pas toujours de définir des politiques d'accès complexes basées sur les attributs des utilisateurs.

Introduction

Limites du chiffrement classique

Le chiffrement classique permet de chiffrer pour un ou plusieurs destinataires précis, mais il devient inefficace lorsqu'il faut gérer un grand nombre d'utilisateurs ou des droits d'accès dynamiques.

Problème : comment contrôler l'accès à une donnée en fonction des attributs d'un utilisateur (rôle, service, département, etc.) sans devoir générer une clé spécifique pour chacun ?

Figure 1 – Exemple de chiffrement symétrique (AES).

Figure 2 – Exemple de chiffrement asymétrique (RSA).

Introduction

Vers le chiffrement basé sur les attributs (ABE)

Pour répondre à ce besoin, le **chiffrement basé sur les attributs** (*Attribute-Based Encryption, ABE*) a été proposé.
Ce mécanisme permet d'associer au texte chiffré ou à la clé des attributs (par exemple "Étudiant", "Professeur", "Informatique"). L'accès aux données est alors conditionné par une **politique d'accès** exprimée logiquement à partir de ces attributs.

2 Principe d'ABE

Principe d'ABE

Définition et concept de base

Le chiffrement basé sur les attributs (Attribute-Based Encryption, ABE) est une extension du chiffrement à clé publique qui permet de contrôler l'accès aux données à l'aide d'attributs.
Le chiffrement et le déchiffrement reposent sur une relation entre un ensemble d'attributs et une politique d'accès, de sorte que seules les entités autorisées peuvent accéder au message.

Principe d'ABE

- Dans le **chiffrement à clé publique**, le chiffrement s'effectue avec une clé publique unique pour un destinataire précis.
- Dans le **chiffrement par attributs**, le chiffrement dépend d'une *politique* d'accès exprimée en termes d'attributs. Ainsi, plusieurs utilisateurs peuvent déchiffrer le message s'ils remplissent la condition.

Exemple

Une donnée chiffrée selon la politique : (Rôle = Enseignant) ET (Département = Informatique) ne sera accessible qu'aux utilisateurs dont la clé contient ces deux attributs.

3 Modèles d'ABE

Modèles d'ABE

Composants principaux d'ABE

- **Autorité de confiance (Trusted Authority) :** génère les paramètres publics du système et distribue les clés secrètes aux utilisateurs en fonction de leurs attributs.
- **Propriétaire des données (Data Owner) :** utilise la clé publique pour chiffrer les données selon une politique d'accès, puis les stocke sur le serveur cloud.
- **Serveur Cloud :** stocke uniquement les données chiffrées sans avoir accès à leur contenu.
- **Utilisateurs des données (Data Users) :** reçoivent une clé secrète associée à leurs attributs et peuvent déchiffrer les données uniquement si leurs attributs satisfont la politique d'accès.

Modèles d'ABE

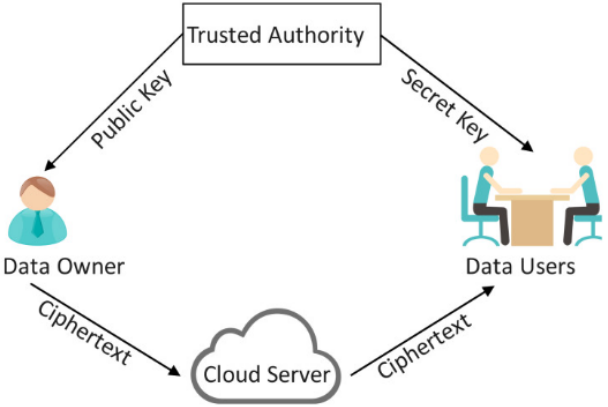

Figure 3 – Architecture de bases d'ABE.

Modèles d'ABE : Key-Policy ABE (KP-ABE)

Dans le modèle **KP-ABE**, la politique d'accès est intégrée dans la **clé privée** de l'utilisateur, tandis que les attributs sont attachés aux données chiffrées.
Ainsi, le chiffreur définit uniquement les attributs du message, et l'autorité décide quelles clés ont le droit de déchiffrer.

Exemple :

Une donnée est chiffrée avec les attributs "Cours=Cryptographie" et "Niveau=3A". Un utilisateur dont la clé contient la politique "(Cours=Cryptographie) ET (Niveau=3A)" pourra la déchiffrer.

Modèles d'ABE : Key-Policy ABE (KP-ABE)

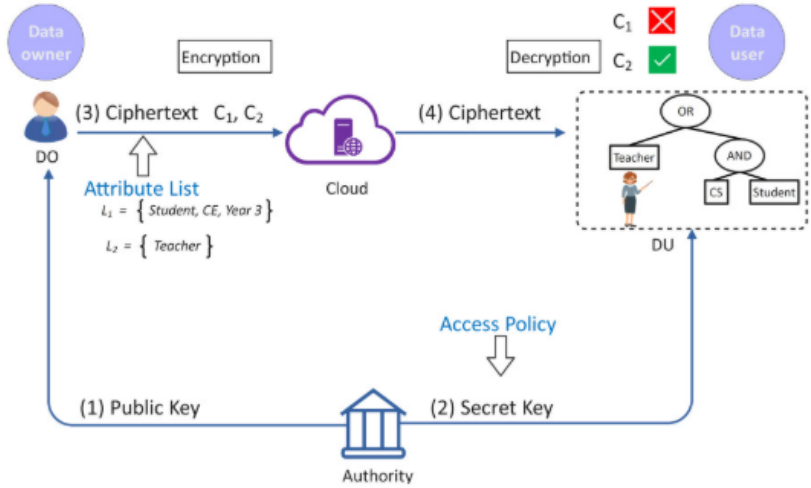

Figure 4 – Processus KP-ABE.

Modèles d'ABE : Ciphertext-Policy ABE (CP-ABE)

Dans le modèle **CP-ABE**, c'est l'inverse : la politique d'accès est intégrée dans le **texte chiffré**, tandis que les attributs appartiennent à la clé de l'utilisateur.
Le chiffreur définit donc directement la condition d'accès.

Exemple :

Une ressource est chiffrée avec la politique "(Rôle = Étudiant) OU (Fonction = Enseignant)".
Tout utilisateur dont la clé contient l'un de ces attributs pourra déchiffrer.

Modèles d'ABE : Ciphertext-Policy ABE (CP-ABE)

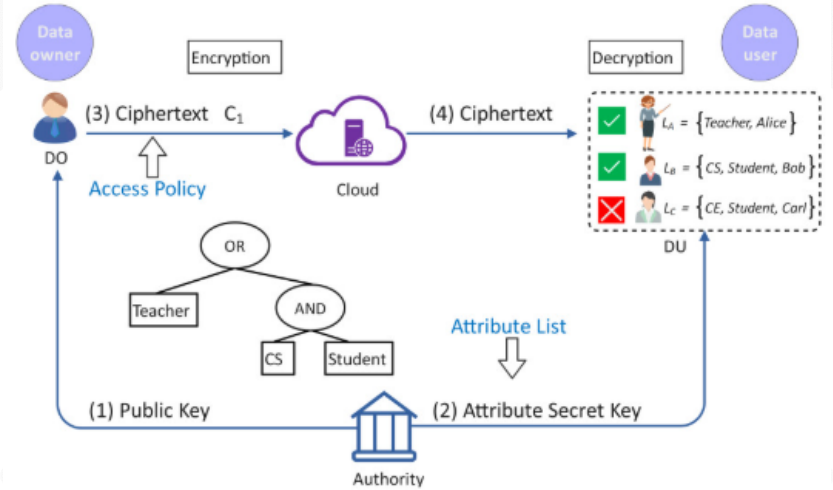

Figure 5 – Processus de CP-ABE.

Modèles d'ABE : Comparaison entre KP-ABE et CP-ABE

Comparaison entre KP-ABE et CP-ABE

Critère	**KP-ABE**	**CP-ABE**
Où est définie la politique ?	Dans la clé de l'utilisateur	Dans le texte chiffré
Qui contrôle l'accès ?	L'autorité	Le chiffreur
Flexibilité du chiffrement	Moyenne	Élevée

4 Domains d'applications d'ABE

Domains d'applications d'ABE

- **Santé** : Contrôle d'accès aux dossiers médicaux selon les attributs comme la spécialité ou le niveau d'autorisation.
- **Éducation** : Gestion de l'accès aux contenus pédagogiques selon le rôle (enseignant, étudiant) ou le département.
- **Cloud computing** : Sécurisation des données stockées en ligne grâce à des politiques d'accès intégrées au chiffrement.
- **Internet des Objets (IoT)** : Limitation de l'accès aux capteurs et dispositifs selon l'emplacement, le type ou la fonction.

5 Conclusion

Conclusion

- Le chiffrement basé sur les attributs (ABE) apporte une solution efficace au problème du contrôle d'accès aux données sensibles.
- Les schémas **KP-ABE** et **CP-ABE** permettent une définition précise et flexible des politiques d'accès.
- Cette approche est particulièrement adaptée aux environnements distribués tels que le **cloud computing** et les systèmes collaboratifs.
- L'ABE renforce la confidentialité des données en intégrant directement les règles d'accès au processus de chiffrement.

Références

- A. Sahai and B. Waters, “Fuzzy Identity-Based Encryption,” EUROCRYPT 2005.
- J. Bethencourt, A. Sahai, B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” IEEE SP 2007.
- D. Boneh, M. Franklin, “Identity-Based Encryption from the Weil Pairing,” 2001.
- https ://www.oaepublish.com/articles/jsss.2023.30

Merci pour votre attention !

Avez-vous des questions ?