Knob: Active Revocation Sécurisée et Performante pour des Données Sensibles en Environnement Cloud

Mot clés : Cloud – sécurité – données sensibles – chiffrement – révocation d'accès

Encadrant : Joachim Bruneau-Queyreix – jbruneauqueyreix@enseirb-matmeca.fr

1. Contexte

Dans un contexte où les données sensibles (images satellites, génomes humains, données personnelles etc.) sont stockées dans le cloud, la sécurisation de ces données contre des accès non autorisés devient cruciale. La sécurité repose sur le fait de chiffrer les données avec une clé de chiffrement, et de donner cette dernière aux utilisateurs autorisés uniquement. Cependant, les mécanismes de révocation d'accès, i.e., enlever un droit d'accès à un utilisateur qui le détenait jusqu'alors, sont excessivement coûteux, et posent des défis opérationnels et financiers car ils nécessitent de rechiffrer avec une nouvelle clé les données précédemment chiffrées. A titre d'exemple, révoquer les droits sur plusieurs fichiers dont le volume total est de 4.3TB nécessite environ 7 heures de chiffrement sur 12 serveurs en parallèle.

L'approche Knob, décrite dans l'article "Practical Active Revocation", propose une solution performante et scalable combinant des environnements d'exécution de confiance (TEE) et des transformations cryptographiques comme l'All-or-Nothing Transform (AONT). Cette technique permet de révoquer efficacement l'accès des utilisateurs en ne ré-chiffrant qu'une fraction des données, réduisant drastiquement les coûts de traitement tout en maintenant un haut niveau de sécurité. La révocation ne prend alors que 1 minutes.

2. Objectifs

L'objectif de ce projet est de concevoir une plateforme démontrant l'efficacité et la sécurité d'un mécanisme de révocation active basé sur Knob. Cette plateforme doit être capable de gérer des volumes importants de données tout en garantissant une protection robuste contre les attaques de pré-provisionnement.

Objectifs techniques :

1. Mise en œuvre de l'infrastructure cloud :
   - Déployer un système de stockage cloud (ex. : Apache Cassandra ou AWS S3).
   - Configurer un environnement TEE compatible avec SGX pour exécuter les ré-chiffrements en toute sécurité.
2. Intégration de la transformation All-or-Nothing (AONT) et du mecanisme Knob :
   - Implémenter un pipeline de stockage et de protection des données utilisant AONT
   - Développer les fonctionnalités de ré-chiffrement dans des TEE
   - Optimiser les performances pour traiter efficacement des datasets simulant des cas réels
3. Développement d'une interface de gestion : Créer une interface web permettant aux administrateurs de surveiller les opérations de révocation (ex. : progression, journalisation).

3. Attentes de livrables

1. Prototype fonctionnel : plateforme implémentant Knob avec gestion distribuée des tâches de ré-chiffrement.
2. Démonstrateur interactif : démonstration simulant la révocation d'accès pour un dataset sensible.
3. Évaluation des performances : Comparaison entre Knob et des approches classiques (ré-chiffrement complet) sur des métriques comme le temps de traitement et l'utilisation des ressources.

Profil recherchés

Élèves-ingénieurs ayant de bonnes connaissances en programmation C/C++/python/go et en système et voulant les consolider, et avec une appétence pour le domaine cloud/sécurité/systèmes distribués.