N° d'ordre

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE
CENTRE DE RECHERCHE SUR L'INFORMATION SCIENTIFIQUE ET TECHNIQUE

Mémoire de Post-Graduation Spécialisée en Sécurité Informatique

Thème

Une approche sécurisée de recherche d'informations sur des données cryptées dans un Cloud Computing

Présenté par :

M[lle] Aït Mehdi Samia
M[me] Lehanine Fouzia née Medkour

Devant le jury composé de :

M[me]Nouali Nadia	Directeur de Recherche au CERIST	Président
M. Amira Abdelouahab	Attaché de Recherche au CERIST	Examinateur
M. Saidi Ahmed	Attaché de Recherche au CERIST	Examinateur
M. BoucennaFateh	Attaché de Recherche au CERIST	Encadreur

Promotion 2015

ولم ار في عيوب الناس عيبا كنقص القادرين على التمام
المتنبي

«Les machines un jour pourront résoudre tous les problèmes,mais jamais aucune d'entre elles ne pourra en poser un ! » - Albert Einstein.

REMERCIEMENTS

Ce travail n'aurait pas pu aboutir sans le concours précieux et généreux de notre encadreur*M.BoucennaFateh* dont les compétences avisées en cryptographie nous ont encouragésà traiter le thème du chiffrement homomorphe. C'est avec un énorme plaisir que nous le remercions pour avoir encadré et dirigé ce mémoire, pour nous avoir soutenus et encouragés vu nos légères connaissances sur la cryptographie et notre ignorance totalerelative au chiffrement homomorphe. Nous le remercions pour la disponibilité dont il a fait preuve et pour tous les moyens qu'il a mis à notre disposition pour mener à bien ce projet de fin d'études.

Nous tenons à remercier aussi le Directeur scientifique de la PGS sécurité informatique, *M.Nouali Omar*, pour sa prise en charge en termes d'encadrement de cette formation et ses propositions des thèmes de fin de projets.

Durant notre formation, nous avons eu le privilège de suivre des cours prodiguéspar des enseignants qui se sont distingués par la qualité de leur enseignement, leur expérience et leurs compétences, et tout particulièrement,*M^{me}Benmeziane Souad* Enseignant Chercheur en lui exprimant notre plus profonde gratitude.

Nous tenons également à remercier les membres du jury pour l'intérêt qu'ils ont porté à notre travail, en examinant ce mémoire et pour l'honneur qu'ils nous font en participant à ce jury.

Nous remercions également l'équipe du service formation, particulièrement *M^{me}Sider Karima*, pour leurs aides et leurs disponibilités.

Nous tenons aussi à mentionner le plaisir que nous avons eu de côtoyer les étudiants de la promotion 2014/2015 durant l'année théorique de la PGS Sécurité Informatique, l'échange de connaissances et d'expériences de chacun selon son organisme d'appartenance et son domaine de compétence.

Résumé

Les récents services Cloud offrent une protection fine des données grâce à un chiffrement à la source et à une authentification renforcée, plutôt que de se contenter d'ériger des murs de protection à base de firewalls.
Le chiffrement pratiqué par les fournisseurs de services Cloud nécessite soit le téléchargement de la totalité des données suite à un besoin de l'utilisateur, soit déléguer l'opération de chiffrement et déchiffrement au Cloud. Ces deux options ne peuvent garantir ni performance dans la première, ni sécurité dans la deuxième.
Afin de répondre à ces exigences (performance et sécurité), une nouvelle forme de cryptographie s'est développée, en l'occurrence le chiffrement homomorphe permettant, en gardant les données hébergées dans le Cloud, d'analyser et de traiter l'information sans avoir à la déchiffrer.
L'application du chiffrement homomorphe semble prometteuse dans le domaine de la recherche d'informations sur les données cryptées.
À travers ce projet,nous avons proposé une approche de recherche d'informations cryptées, qui exploitela méthode« LeveledFullyhomomorphicEncryption » proposée par Brakerski, Gentry et Vaikuntanathan en 2012,et nous l'avons implémenté en utilisant la librairie (HElib)écrite en C++par Halevi et Shoup.

Mots-clés : Chiffrement Homomorphe, Recherche d'Information Cryptée, Cloud Computing

Abstract

New Cloud services offer a thin data protection through encryption at source and strong authentication, rather than erecting protective walls based on firewalls.

Encryption performed by Cloud services providers requires either downloading all data to meet a user needs. Or delegate the encryption and decryption to the Cloud. These two options cannot guarantee performance in the first and security in the second.

In order to meet these requirements (performance and security), a new form of cryptography has been developed, known as homomorphic encryption, that allows processing information without having to decipher them.

The application of homomorphic encryption seems promising in information retrieval over encrypted data.

Through this project, we suggested an encrypted information retrieval approach that uses "LeveledFullyhomomorphicEncryption" schemeproposed by Brakerski, Gentry and Vaikuntanathan in 2012, and we have implemented it using the library (HElib) written in C ++ by Halevi and Shoup.

Key words: Homomorphic Encryption, Information Retrieval Over Encrypted Data, Cloud Computing

Table des matières