REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ SAAD DAHLAB BLIDA

Faculté des Sciences
Département : Informatique

Mémoire de fin d'étude pour l'obtention du diplôme de Master en Informatique
OPTION : Sécurité des Systèmes d'Information

Présenté par :
HELAL Sonya

Thème

Authentification Anonyme et Contrôle d'Accès dans un Environnement Cloud : Application au Domaine e-santé

Organisme d'accueil: Centre de Recherche sur l'Information Scientifique et Technique (CERIST)

Soutenu le 29/09/2019 devant le jury composé de :

Mme Toubaline	**Présidente**
Mme Ghebghoub	**Examinatrice**
Mme AROUSSI Sana	**Promotrice**
Mrs SAIDI Ahmed	**Encadreur**

Promotion : 2018-2019

Remerciement

*Mes remerciements, avant tout, à **DIEU** tout puissant pour la volonté, la santé et la patience qu'il m'a données durant toutes ces longues années d'études afin que je puisse arriver à ce stade.*

Je remercie mes très chers parents qui ont toujours été là pour moi, « Vous avez tout sacrifié pour vos enfants n'épargnant ni santé ni efforts. Vous m'avez donné un magnifique modèle de labeur et de persévérance. Je suis redevable d'une éducation dont je suis fier ». Je remercie également mon frère Salim, et mes sœurs Sara et Soraya pour leur encouragement.

Je tiens à exprimer toute ma reconnaissance à mon encadreur Madame AROUSSI Sana. Je la remercie pour sa disponibilité et la confiance qu'elle m'a accordée. J'aimerais aussi la remercier pour les soutiens et ses précieux conseils qui m'ont permis de mener à bien ce travail. Je ne la remercierai jamais assez, qu'elle trouve en ce mémoire l'expression de ma profonde gratitude et mon respect infini.

Je remercie tout particulièrement Monsieur SAIDI Ahmed, attaché de recherche au CERIST, promoteur de thèse, de m'avoir orienté, corrigé mon travail et encouragé. Merci pour sa disponibilité et sa gentillesse sans égale. J'ai profité pendant longtemps du savoir et du savoir-faire dont j'ai pu bénéficier au cours de nombreuses discussions.

Je remercie également le service Formation du CERIST de nous avoir prodigué un excellent environnement de travail.

J'adresse mes sincères remerciements à tous les professeurs, intervenants et toutes les personnes qui par leurs paroles, leurs écrits, leurs conseils et leurs critiques ont guidé mes réflexions et ont accepté à me rencontrer et répondre à mes questions durant mes recherches.

Je remercie le membre de jury pour m'avoir fait l'honneur de juger mon travail.

Afin de n'oublier personne, mes vifs remerciements s'adressent à tous ceux qui m'ont aidée à la réalisation de ce modeste mémoire

Tout simplement Merci !

Dédicace

Je dédie ce modeste travail en signe de respect, reconnaissance et de remerciement :

A mes chers parents, qui ne cessent de me donner avec amour le nécessaire pour que je puisse arriver à ce que je suis aujourd'hui. Que dieux vous protège et que la réussite soit toujours à ma portée pour que je puisse vous combler de bonheur.

A mes chers sœurs Sara et Soraya ainsi qu'à mon frère Salim, en reconnaissance de leur affection toujours constante

Tous mes proches

Tous mes amis, mes collègues et tous ceux qui m'estiment.

Résumé

Le cloud computing, ou informatique en nuage est une technologie qui a connu un développement rapide aux cours de ces dernières années. D'un point de vue sécurité de l'information, un certain nombre de questions se posent sur les différentes menaces que font face le Cloud, notamment la confidentialité des utilisateurs et l'intégrité des données stockées. L'objectif de ce mémoire est de mettre en place des solutions à ces deux problématiques dans le cadre de domaine de e-santé.

Pour ce faire, nous avons développé deux méthodes dont chacune fait l'objet d'une contribution. La première contribution fournit un modèle de contrôle d'accès basé sur la méthode de chiffrement à base d'attribut CP ABE, qui permet aux propriétaires de données de garantir la sécurité des données et de fournir aux utilisateurs un accès fin aux données en utilisant des politiques et des contraintes définies. La seconde contribution fournit une authentification anonyme qui est l'une des solutions qui peuvent être utilisées pour préserver la confidentialité des données personnelles c'est-à-dire qu'elle rend les identités des utilisateurs anonyme une fois qu'ils s'authentifient au sein du cloud. Les résultats expérimentaux de notre solution montrent que ces deux méthodes sont efficaces pour gérer en toute sécurité les données stockées dans le cloud et assure la confidentialité des utilisateurs.

Mots – clés : Sécurité cloud computing, confidentialité, intégrité de données, Chiffrement CP-ABE, e-santé, Contrôle d'accès, Authentification anonyme.

Abstract

Cloud computing is a technology that has grown rapidly in recent years. From an information security perspective, a number of questions arise about the various threats facing the cloud, including user privacy and the integrity of stored data. The objective of this thesis is to implement solutions to these two problems within the framework of the e-health domain.

To do this, we have developed two methods, each of which is the subject of a contribution. The first contribution provides an access control model based on the CP ABE attribute-based encryption method, which allows data owners to ensure data security and provide users with fine access to data using defined policies and constraints. The second contribution provides anonymous authentication, which is one of the solutions that can be used to preserve the confidentiality of personal data, i.e. it makes users' identities anonymous once they authenticate in the cloud. The experimental results of our solution show that both methods are effective in safely managing data stored in the cloud and ensuring user confidentiality.

Key – words: Cloud computing security, confidentiality, data integrity, CP-ABE encryption, e-health, access control, anonymous authentication.

ملخص

الحوسبة السحابية هي تقنية شهدت تطوراً سريعاً في السنوات الأخيرة. من منظور أمن المعلومات ، يطرح عدد من الأسئلة حول التهديدات المختلفة التي تواجه السحابة ، بما في ذلك خصوصية المستخدم وسلامة البيانات المخزنة. الهدف من هذه الرسالة هو تنفيذ حلول لهاتين المشكلتين في إطار مجال الصحة الإلكترونية.

للقيام بذلك ، قمنا بتطوير طريقتين ، كل منها موضوع مساهمة. توفر المساهمة الأولى نموذج التحكم في الوصول استنادًا إلى طريقة التشفير المعتمدة على سمة CP ABE ، والتي تتيح لأصحاب البيانات ضمان أمان البيانات وتزويد المستخدمين بوصول جيد إلى البيانات باستخدام سياسات وقيود محددة. توفر المساهمة الثانية مصادقة مجهولة المصدر ، وهي أحد الحلول التي يمكن استخدامها للحفاظ على سرية البيانات الشخصية ، أي أنها تجعل هويات المستخدمين مجهولة بمجرد المصادقة في السحابة. توضح النتائج التجريبية لحلنا أن كلتا الطريقتين فعالتين في إدارة البيانات المخزنة في السحابة بأمان وضمان سرية المستخدم.

الكلمات – المفتاحية: أمان الحوسبة السحابية ، السرية ، تكامل البيانات ، تشفير CP-ABE ، الصحة الإلكترونية ، التحكم في الدخول ، المصادقة المجهولة.

Table des matières