



AVIS DE SOUTENANCE THESE DE DOCTORAT

Présentée par

Mr : IMAD EL GHOUBACH

Discipline : Informatique

Spécialité : Informatique

Sujet de la thèse : La sécurité des données dans le Cloud Computing.

Formation Doctorale : Sciences de l'ingénieur Sciences Physiques, Mathématiques et Informatique.

Thèse présentée et soutenue le mercredi 15 juillet 2020 à 16h au centre de Conférences devant le jury composé de :

Nom Prénom	Titre	Etablissement	
Arsalane ZARGHILI	PES	Faculté des Sciences et Techniques Fès	Président
Sabir ESSAID	PH	Ecole Nationale Supérieure d'Electricité et Mécanique Casablanca	Rapporteur
Hussain BEN-AZZA	PH	Ecole Nationale Supérieure d'Arts et Métiers Meknès	Rapporteur
Azeddine ZAHI	PH	Faculté des Sciences et Techniques Fès	Rapporteur
Said NAJAH	PH	Faculté des Sciences et Techniques Fès	Examineur
Khalid ZENKOUAR	PH	Faculté des Sciences et Techniques Fès	Examineur
Fatiha MRABTI	PH	Faculté des Sciences et Techniques Fès	Directeurs de thèse
Rachid BEN ABOU	PH	Faculté des Sciences et Techniques de Fès	

Laboratoire d'accueil : laboratoire Systèmes Intelligents et Applications.

Etablissement : Faculté des Sciences et Techniques de Fès.



Titre de la thèse : La sécurité des données dans le Cloud Computing.

Nom du candidat : IMAD EL GHOUBACH

Spécialité : Informatique

Résumé de la thèse

Le cloud computing s'est largement développé au cours de ces dernières années. Cette technologie a acquis une grande popularité dans le domaine informatique. Ceci revient à la capacité des fournisseurs de cloud d'assurer une évolutivité et des ressources « infinies » avec un accès distribué et à la demande. L'accès à distance aux services Cloud permet aux utilisateurs du cloud de négliger l'existence de l'infrastructure informatique derrière. En raison de la virtualisation et de la multi-location, l'infrastructure cloud devient de plus en plus complexe et invisible par rapport aux centres de données traditionnels. Cette ambiguïté rend la gestion de la fourniture des services, la surveillance, la sauvegarde, la reprise après incident et en particulier la gestion de sécurité plus compliquée. Pour cette raison, il y a un manque croissant de confiance dans les infrastructures cloud.

Cette dissertation vise à surmonter ce dilemme, tout en tenant compte de deux préoccupations de sécurité des données, à savoir la confidentialité des données et l'intégrité des données.

En premier lieu, nous nous focalisons sur le problème de confidentialité des données, un enjeu assez compliqué à cause du partage de données flexible dans un groupe dynamique d'utilisateurs. Pour répondre à cette préoccupation, nous avons, d'une part, proposé une nouvelle amélioration d'une méthode P2E, reposant sur l'utilisation de la cryptographie basée sur les attributs, où nous avons étudié l'impact de l'utilisation d'une structure d'accès plus générale sur la performance et l'évolutivité de partage. Grâce aux propriétés de la structure d'accès à seuil, cette contribution a démontré sa capacité de gérer des accès assez complexes, tout en ayant un impact négligeable sur la performance. D'autre part, nous définissons ESS-ODER, une solution à base de cryptographie basée sur les attributs, qui propose la délégation de la tâche de déchiffrement vers un serveur proxy pour répondre à la limitation de certains terminaux, à puissance limitée, utilisées. En effet, ESS-ODER permet un partage sécurisé des données dans un environnement cloud tout en maintenant une gestion de contrôle d'accès flexible.

Deuxièmement, nous abordons le problème de la preuve de possession de données (PDP). En fait, le client cloud doit disposer d'une méthode efficace pour effectuer des vérifications d'intégrité périodiques à distance sans conserver les données localement.

Afin de satisfaire à cette exigence de sécurité, nous définissons SERDAS, une solution basée sur le chiffrement basé sur l'identité, permettant l'utilisateur de déléguer, d'une manière sécurisée, la vérification de ses données à un auditeur tiers. Cette méthode offre un garant probabiliste d'intégrité des données tout en ayant un nombre illimité de vérification.

Mots clés : Cloud Computing ; Stockage sécurisé des données ; Confidentialité ; Intégrité ; Chiffrement basé sur les attributs ;