SOUTENANCE DE THÈSE

M. Youcef Imine

Soutiendra sa thèse de **Doctorat** sur le sujet :

Cloud computing security

Dans l'Unité de Recherche **:**

HEUDIASYC UMR CNRS 7253

Lundi 18 novembre 2019 à 9h30

à l'UTC, centre Pierre Guillaumat, amphi L103

devant le jury composé de :

M^me^ Francine Krief, professeur, Bordeaux INP, LABRI
M. Ahmed Serhrouchni, professeur, Télécom-Paristech, Paris
M. Bijan Jabbari, professeur, George Mason University, Fairfax, États-Unis,
M^me^ Isabelle Christment, professeur, LORIA, Vandœuvre-lès-Nancy
M. Romain Laborde, maître de conférences, université de Toulouse, IRIT3
M. Walter Schön, professeur, université de technologie de Compiègne, laboratoire Heudiasyc
M. Abdelmadjid Bouabdallah, professeur des universités, université de technologie de Compiègne, laboratoire Heudiasyc

Abstract:

These last years, we are witnessing a real digital revolution of Internet where many innovative applications such as Internet of Things, autonomous cars, etc., have emerged. Consequently, adopting externalization technologies such as cloud and fog computing to handle this technological expansion seems to be an inevitable outcome. However, using the cloud or fog computing as a data repository opens many challenges in prospect.

This thesis addresses security issues in cloud and fog computing which is a major challenge that need to be appropriately overcome. Indeed, adopting these technologies means that the users lose control over their own data, which exposes it to several security threats. Therefore, we first investigated the main security issues facing the adoption of cloud and fog computing technologies.
As one of the main challenges pointed in our investigation, access control is indeed a cornerstone of data security. An efficient access control mechanism must provide enforced and flexible access policies that ensure data protection, even from the service provider. Hence, we proposed a novel secure and efficient attribute-based access control scheme for cloud data-storage applications. Our solution ensures flexible and fine-grained access control and prevents security degradations. Moreover, it performs immediate users and attributes revocation without any key regeneration.
Authentication service in fog computing architecture is another issue that we have addressed in this thesis. Some traditional authentication schemes endure latency issues while others do not satisfy fog-computing requirements such as mutual authentication between end-devices and fog servers. Thus, we have proposed a new, secure and efficient authentication scheme that ensures mutual authentication at the edge of the network and remedies to fog servers' misbehaviors.

Finally, we tackled accountability and privacy-preserving challenges in information-sharing applications for which several proposals in the literature have treated privacy issues, but few of them have considered accountability service.
Therefore, we have proposed a novel accountable privacy-preserving solution for public information sharing in data externalization platforms. Externalization servers in our scheme authenticate any user in the system without violating its privacy.
In case of misbehavior, our solution allows to trace malicious users thanks to an authority.

Keywords: Cloud computing, fog computing, security, access control, revocation, authentication, privacy, accountability.

Résumé:

Ces dernières années, nous assistons à une immense révolution numérique de l'Internet où de nombreuses applications innovantes telles que l'Internet des objets, les voitures autonomes, etc., ont émergées. Par conséquent, l'adoption des technologies d'externalisations des données, telles que le cloud ou le fog computing, afin de gérer cette expansion technologique semble inévitable. Cependant, l'utilisation du cloud ou du fog computing en tant que plateforme d'externalisation pour le stockage ou le partage des données crée plusieurs défis scientifiques. En effet, externaliser ses données signifie que l'utilisateur perd le contrôle sur ces derniers. D'où, la sécurité des données devienne une préoccupation majeure qui doit être proprement traitée. C'est dans ce contexte que s'inscrivent les travaux de cette thèse dans laquelle nous avons déterminé dans un premier temps les principaux problèmes de sécurité liés à l'adoption du cloud et du fog computing.

Le contrôle d'accès aux données est l'un des défis majeurs que nous avons identifié. Un mécanisme de contrôle d'accès efficace doit permettre d'appliquer des politiques d'accès fiables, flexibles et qui garantissent la protection des données contre toute sorte d'accès non autorisé venant des utilisateurs ou du fournisseur de service. De ce fait, nous avons proposé une nouvelle solution de contrôle d'accès basée sur le chiffrement à base d'attributs pour les applications de stockage de données dans le cloud. Notre solution assure un contrôle d'accès souple et à grains fins. De plus, elle permet d'effectuer une révocation immédiate des utilisateurs et des attributs sans aucune mise à jour des clés de chiffrement fournies aux utilisateurs. Le service d'authentification dans une architecture fog computing est un autre problème que nous avions abordé durant cette thèse. En effet, certains schémas traditionnels d'authentifications proposés dans la littérature sont confrontés à des problèmes de latence, tandis que d'autres ne sont pas conformes aux exigences du fog computing telles que l'authentification mutuelle entre les utilisateurs et les serveurs Fog. Ainsi, nous avons proposé un nouveau schéma d'authentification efficace, qui assure l'authentification mutuelle et qui est robuste contre les comportements malicieux des serveurs Fog.

Enfin, nous avons abordé le problème de traçabilité et de la protection de la vie privée dans le cadre des applications de partage d'informations publiques. Plusieurs propositions dans la littérature ont traité les problèmes liés à la protection de la vie privée. Cependant, peu de solutions ont envisagé un service de traçabilité. Par conséquent, nous avons proposé une nouvelle solution pour le partage d'informations publiques assurant le service de traçabilité tout en préservant les informations privées des utilisateurs. Avec notre solution, les serveurs d'externalisations authentifient les utilisateurs sans pouvoir obtenir des informations sur leur vie privée. En cas de comportements malicieux, notre solution permet de tracer les utilisateurs malveillants grâce à une autorité.

Mots clés : Cloud computing, fog computing, contrôle d'accès, révocation, authentification, vie privée, traçabilité.