AVIS DE PRESENTATION DE THESE EN SOUTENANCE POUR L'OBTENTION DU DIPLOME NATIONAL DE DOCTEUR

Monsieur Van-Hoan HOANG

Présentera ses travaux intitulés :

« Sécurisation des accès et des échanges dans un écosystème hétérogène d'utilisation des contenus en mobilité : Une approche adaptative et sensible au contexte »

Spécialité : Informatique et applications

Le 27 janvier 2022 à 14h00

Lieu :

CertEurope
41, rue de l'échiquier
75010 Paris

Composition du jury :

Mme BOUZEFRANE Samia	**Professeure, CNAM**
Mme CHAHOUCHI Hakima	**Professeure, Télécom SudParis**
M. CUPPENS Frédéric	**Professeur, Polytechnique Montréal**
M. GHAMRI-DOUDANE Yacine	**Professeur, La Rochelle Université**
M. LEHTIHET Elyes	**Innovation Manager, OODRIVE**
M. SAUVERON Damien	**Maître de conférences, HDR, Université de Limoges**
M. SERHROUCHNI Ahmed	**Professeur, Télécom Paris**
M. ZEMMARI Akka	**Professeur, Université de Bordeaux**

Résumé :

Les services de stockage et de partage de données basés sur le Cloud sont largement adoptés depuis des décennies. Le modèle sous-jacent permet aux utilisateurs de minimiser le coût de services en étant en mesure d'accéder et de partager des données facilement. Dans ce contexte, la sécurité est essentielle pour protéger des utilisateurs et leurs ressources. Concernant les utilisateurs, ils doivent prouver leur éligibilité pour pouvoir accéder aux ressources. Cependant, l'envoi direct des informations personnelles permet aux fournisseurs de services de détecter qui partage des données avec qui et de corréler leurs activités. Quant aux données, en raison de la complexité du déploiement d'un système de gestion de clés, elles ne sont pas chiffrées par les utilisateurs mais par les fournisseurs de services. Cela leur permet de les lire en clair.

Dans la thèse, nous créons tout d'abord un protocole d'authentification et d'échange de clés basé sur un mot de passe qui permet de sécuriser des échanges entre des utilisateurs et des fournisseurs de services. Deuxièmement, nous construisons une PKI décentralisée qui permet de créer des protocoles d'authentification en préservant la vie privée des utilisateurs. Troisièmement, nous concevons deux schémas de chiffrement à base d'attributs. Ces schémas fournissent des systèmes de gestion de clés efficaces pour protéger des données en conservant la capacité de les partager avec d'autres. Enfin, nous construisons une plateforme de partage de données en tirant parti de la technologie blockchain. La plateforme garantit une haute disponibilité, la confidentialité des données, un contrôle d'accès sécurisé, et la vie privée des utilisateurs.