IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

AVIS DE SOUTENANCE DE THESE

COLLEGES SCIENCES
BRETAGNE POUR L'INGENIEUR
LOIRE ET LE NUMERIQUE

M. Kouadio Rodrigue N'GORAN

Département INFO - laboratoire Lab-STICC

Soutiendra publiquement ses travaux en vue de l'obtention du grade de

Docteur d'IMT Atlantique

Dans le cadre de la co-accréditation de thèse d'IMT Atlantique au sein de l'école doctorale SPIN en cotutelle

avec Institut National Polytechnique Félix Houphouët-Boigny (INPHB)

Le 15/12/2023 à 14h00 à IMT Atlantique, campus de Brest

B 03-036

Pour assister à la soutenance, connectez-vous à l'adresse : https://imt-

atlantique.webex.com/imt- atlantique/j.php?MTID=mecaad1e3b3fa6fe99c5c96a67bdb219b

Stratégie de sécurité Zero Trust dans un environnement de cloud communautaire

Résumé : De nos jours, la société est caractérisée par une mobilité importante des populations et des besoins croissants en termes de partage de gros volumes de données sensibles au sein des entreprises et de collaboration avec des organisations partenaires ou concurrentes. Ces collaborations procurent de nombreux avantages aux entreprises en termes d'évolutivité et de croissance économique. Cependant, les systèmes informatiques de ces organisations sont exposés à divers types de menaces et cyberattaques de plus en plus sophistiquées. Les stratégies traditionnelles de sécurisation des infrastructures fondées sur le périmètre ne sont plus suffisantes. Le modèle de sécurité Zero Trust est une approche de cybersécurité qui considère toutes les entités d'une infrastructure comme potentiellement vulnérables en tout temps et en tout lieu. Cette stratégie se positionne comme une réponse à la problématique de sécurisation de ces systèmes hétérogènes, complexes, dynamiques et distribués. Cependant, sa mise en œuvre varie en fonction du contexte du système, et exige des changements organisationnels et culturels. En effet, les systèmes de collaboration sont caractérisés par la nécessité de garantir l'autonomie des entités engagées, la confiance entre elles et le besoin de protection des informations sensibles de diverses natures échangées. Dans cette thèse, nous proposons, une stratégie de sécurité Zero Trust dans un contexte de collaboration entre des organisations au sein d'un cloud communautaire. Le modèle présente une architecture hiérarchique pour sécuriser les échanges au sein et entre des organisations. Il fournit un système de gestion décentralisée des identités des utilisateurs et des organisations grâce aux identifiants décentralisés et aux informations d'identifications vérifiables. Cette méthode expose un moyen d'authentification continue des entités et de stockage des données dans un registre distribué de type blockchain. Par ailleurs, la démarche propose une technique d'évaluation de la confiance entre les organisations. En outre, la stratégie inclut un mécanisme de spécification de règles de politique d'accès et de suivi de contrat de collaboration. Des expérimentations ont été menées afin de prouver l'efficacité et la fiabilité des mécanismes proposées, fournissant ainsi une architecture et des mesures de sécurité associées pour le déploiement d'une stratégie Zero Trust dans un environnement de collaboration.

Mots-clés: Zero Trust, Confiance, identités décentralisées, Blockchain, Contrôle d'accès, Cloud communautaire

Le jury est composé de :

M. Yvon KERMARREC	- Professeur	- IMT Atlantique
M. Olivier Pascal ASSEU	- Professeur	- ESATIC, Côte d'Ivoire
M. Jean-Louis TETCHUENG	- Chargé d'enseignement	- Orange Labs Rennes
M. Christophe CLARAMUNT	- Professeur	- École navale
Mme Jamal EL HACHEM	- Maître de conférences	- Université de Bretagne Sud
M. Hyacinthe KONAN	- Maître de conférences	- Institut National Polytechnique H Boigny
M. Frédéric CUPPENS	- Professeur	- Polytechnique Montréal

M. Jérémy BUISSON - Maître de conférences - École de l'Air et de l'Espace