Stage M2

Un méta-modèle ou une ontologie des bonnes pratiques pour assurer la sécurité du Cloud

L'équipe DiverSE : Inria/Irisa DiverSE Team
Encadrant 1: Stéphanie Challita
Email : stephanie.challita@irisa.fr
Encadrant 2: Nan Zhang Messe
Email : nan.zhang@univ-rennes1.fr
Encadrant 3: Olivier Barais
Email : olivier.barais@irisa.fr

Mots Clés :

Sécurité du Cloud, Google Cloud Platform (GCP), AWS, Azure, API, Ontologie, Méta-modèle, Patron de sécurité, Bonne pratique concernant les contre-mesures, NLP

Contexte et Problématique :

Bien que de nombreuses personnes ne connaissent pas l'informatique en nuage ou Cloud, elles l'utilisent dans leur vie quotidienne via les réseaux sociaux, le courrier électronique, la messagerie instantanée, etc. La technologie du Cloud fournit une architecture de système innovante qui tend à transformer le modèle informatique traditionnel en un modèle de services. Ce nouveau modèle modifie la façon dont les ressources du système sont allouées, la manière dont les données sont stockées et aussi la manière dont les utilisateurs ont accès à leurs données en raison des caractéristiques du Cloud. Ces caractéristiques ont été identifiées par de nombreux chercheurs, on en cite : la virtualisation, le multi-tenancy, l'élasticité et l'évolutivité, l'indépendance du dispositif et de l'emplacement. Ainsi, les utilisateurs finaux d'une infrastructure en Cloud sont capables de bénéficier de nombreux avantages découlant de ces caractéristiques [1].

Toutefois, ces mêmes caractéristiques introduisent de nouveaux problèmes de sécurité, de sorte que les nouveaux utilisateurs sont découragés de déménager dans le Cloud. Plusieurs défis de la sécurité sont cités dans la littérature : la confidentialité, l'intégrité et la disponibilité des données, l'authentification et l'autorisation, les vulnérabilités de la virtualisation, et l'attaque par ingénierie sociale, etc [2]. Il existe des travaux concernant l'ontologie ou le méta-modèle qui structurent des connaissances dans le domaine de la sécurité du Cloud [3], mais ces travaux sont plutôt orientés vers le côté d'attaque. Du côté de la bonne pratique ou la protection, à ce jour-là, il n'y a pas encore une ontologie proposée.

Objectif :

L'objectif de ce stage est de proposer une ontologie ou un méta-modèle des bonnes pratiques pour assurer la sécurité du Cloud. Cette ontologie devrait à la fin guider les développeurs à choisir des moyens plus sécurisés lors de la conception et de l'implémentation des applications Cloud. Pour faire cela, il faut étudier des patrons des

bonnes pratiques de sécurité ou des contre-mesures correspondant à chaque problème de sécurité dans le Cloud et les représenter sous forme d'ontologie ou de méta-modèle. Ces bonnes pratiques peuvent être extraites depuis des API stables comme par exemple Google Cloud Platform, et le méta-modèle produit sera validé par d'autres APIs comme Amazon Web Services (AWS) et Microsoft Azure.

Ensuite, il faut concevoir et développer un outil de support ou une librairie basée sur ce méta-modèle qui permet de détecter automatiquement des mauvaises pratiques qui engendrent des vulnérabilités de l'application Cloud, et qui propose de les corriger par la suite, dans le but d'aider les développeurs à concevoir et implémenter les services Cloud de manière sécurisée.

Environnement :

Le candidat travaillera au sein de l'équipe de DiverSE, Inria. Inria est un institut national français de recherche en informatique, 8 centres de recherche sont situés dans toute la France, accueillant plus de 200 équipes de recherche. L'équipe de DiverSE est située à Rennes. La recherche de DiverSE est dans le domaine de l'ingénierie logicielle. L'équipe participe activement à des projets européens, français et industriels et se compose de 9 membres du corps professoral, 20 doctorants, 2 post-docs et 4 ingénieurs. Le candidat travaillera dans le contexte d'une thématique actuellement explorée dans l'équipe, impliquant divers professeurs et étudiants.

Compétences Requises :

- Capacité à travailler de manière autonome
- Passionné pour le développement de logiciels
- Forte expertise en Java
- Connaissance du Cloud Computing, du traitement du langage naturel et de l'ingénierie dirigée par les modèles est un plus
- Capacité à écrire et à communiquer oralement, de préférence en anglais puisque DiverSE accueille de nombreux doctorants étrangers, des post-docs et des chercheurs invités

Références :

[1] Pattakou, Argyri et al. "Reasoning About Security and Privacy in Cloud Computing Under a Unified Meta-Model." *HAISA* (2016).
[2] Ritesh Sharma, Mahendra Kumar Gourisaria, and S. S. Patra. "Cloud Computing — Security, Issues, and Solutions.", Proceedings of INDIA 2019, Communication Software and Networks.
[3] Xia, T. et al. "Metamodel for Security and Privacy Knowledge in 1 Cloud Service Development 1 2." MODELSWARD (2019).