Université de Rennes

Appel à projets - Année 2026

Contrats doctoraux «Ordinaires»

Direction de la Recherche et de l'Innovation

ECOLE DOCTORALE : MATISSE **POLE DE RECHERCHE : Mathématiques-numérique**

Unité de recherche d'accueil

Unité de Recherche : IRISA, UMR 6074

Equipe : DiverSE

Encadrement

Directeur de thèse : Olivier Barais **Unité de recherche** : IRISA

Employeur/Établissement d'origine : Université de Rennes

HDR : ☒ oui • non **Nb de thèses en cours** : 6

Mail : olivier.barais@irisa.fr **Tél**. : 0667605935

Encadrante : Stéphanie Challita **Unité de recherche** : IRISA

Employeur/Établissement d'origine : Université de Rennes

HDR : • oui ☒ non **Nb de thèses en cours** : 1

Mail : stephanie.challita@irisa.fr **Tél.** : 0754531840

Sujet

Titre : Privacy-Compliant REST APIs

Mots clés : REST API, OpenAPI, Model-Driven Engineering, Privacy

Cotutelle internationale (oui/non) : Non **Si oui, préciser l'établissement et le pays de rattachement** :

Descriptif (15-30 lignes) :
Contexte socioéconomique et scientifique ; Les hypothèses et questions posées ; Les grandes étapes de la thèse et démarche ; Approches méthodologiques et techniques envisagées

Contexte

Les API REST constituent aujourd'hui un pilier de l'économie numérique, en particulier dans des domaines sensibles tels que la santé, les services publics ou le cloud computing. Elles exposent des données personnelles à grande échelle, mais leur conception repose souvent sur des spécifications incomplètes ou imprécises, ce qui engendre des risques importants en matière de confidentialité et de conformité réglementaire. En pratique, **des incohérences entre les spécifications, les implémentations et les exigences légales peuvent conduire à des violations du RGPD, telles que la surexposition de données, des usages non conformes ou des accès non autorisés.**

Hypothèses

Les objectifs de cette thèse sont formulés par les questions de recherche suivantes :

QR1 : Comment identifier systématiquement les risques liés à la confidentialité dans les API REST au niveau des spécifications, en particulier pour l'exposition et le traitement des données personnelles ?

QR2 : Comment représenter explicitement les données personnelles et les contraintes réglementaires (minimisation, limitation des finalités, restrictions d'accès) dans les spécifications d'API pour prévenir tout usage ou exposition non intentionnel ?

QR3 : Dans quelle mesure l'analyse au niveau des spécifications permet-elle de détecter et réduire les violations du RGPD avant le déploiement ?

Démarche scientifique

Une première phase consistera en une **étude empirique à grande échelle de spécifications d'API REST** issues de sources ouvertes et largement utilisées (Software Heritage, GitHub, APIs.guru), **afin d'identifier des motifs récurrents d'incohérences, de mauvaises pratiques et de risques liés à la confidentialité.** Cette analyse permettra de mieux comprendre les limites des spécifications existantes et de caractériser les types de risques les plus fréquents. Sur la base de ces observations, la thèse proposera la **définition d'un cadre de modélisation fondé sur l'ingénierie dirigée par les modèles (Model-Driven Engineering), plaçant les spécifications OpenAPI au cœur du raisonnement sur la protection**

des données et la conformité réglementaire. Ce cadre enrichira les spécifications par des informations explicites sur les données personnelles et les règles de confidentialité, et servira de support au développement de **mécanismes automatisés d'analyse, de vérification et de test orientés confidentialité.** Ces mécanismes seront intégrés dans des **chaînes d'intégration et de déploiement continus pour assurer une prise en compte systématique et continue des exigences de protection des données tout au long du cycle de vie des API.**

Méthodologie et techniques

La thèse combinera plusieurs approches complémentaires : analyse empirique de spécifications existantes, modélisation formelle, transformations de modèles et développement d'outils automatisés. Les solutions développées seront évaluées sur des API open source et industrielles afin d'en mesurer la robustesse, la scalabilité et l'efficacité dans l'identification et la réduction des risques de non-conformité, tout en démontrant leur pertinence pour la conception et la maintenance d'API REST respectueuses de la vie privée.

Liste de publications

1. A. Cavoukian, 2009. *Privacy by Design: The 7 Foundational Principles.* Information and Privacy Commissioner of Ontario, Canada.
2. T. Antignac et al., 2018. *Privacy Compliance Via Model Transformations.* IEEE European Symposium on Security and Privacy Workshops (EuroS&P Workshops).
3. S. Krstić et al., 2024. *Model-Driven Privacy.* PETS.
4. B.O. Emeka et al., 2023. *A Practical Model Driven Approach for Designing Security Aware RESTful Web APIs Using SOFL.* IEICE TRANSACTIONS on Information and Systems.
5. **S. Challita** et al., 2018. A Precise Model for Google Cloud Platform. IEEE IC2E.
6. H. Cao et al., 2017. *Automated Generation of REST API Specification from Plain HTML Documentation.* ICSOC.
7. E. Grünewald et al., 2021. *TIRA: an OpenAPI Extension and Toolbox for GDPR Transparency in RESTful Architectures.* IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).
8. A. El fraihi et al., 2024. Client-side and Server-side Tracking on Meta: Effectiveness and Accuracy. PETS.