Sujet de Stage

Titre : Conception d'un système d'échange de données sécurisé pour les acteurs d'une chaîne d'approvisionnement en matières premières et services critiques.

Contexte :
Dans le monde globalisé d'aujourd'hui, la supply chain joue un rôle crucial dans la réussite des entreprises, en assurant un flux continu de biens et de services du producteur au consommateur. Cependant, cette chaîne de valeur étendue est confrontée à des défis majeurs en matière de sécurité des données, en raison de la nécessité d'échanger des informations sensibles entre divers intervenants. Avec l'augmentation des cyberattaques et des exigences réglementaires strictes pour la protection des données, il devient impératif de trouver des solutions innovantes pour sécuriser ces échanges.
Différentes techniques cryptographiques dont les Zero Knowledge Proofs (ZKP) peuvent répondre à ce défi. Ces techniques, associées à la technologie blockchain offrent une solution robuste qui va sécuriser la manière dont les données sont partagées sur la supply chain en assurant la confidentialité et la sécurité des informations échangées.

Objectif :
L'objectif de ce stage est de développer et d'implémenter une solution basée sur les tokens associés à des techniques cryptographiques pour faciliter l'échange sécurisé de données entre les différents acteurs d'une supply chain en général. Cette brique technologique pourra être appliquée dans différents cas d'usages dont la chaîne d'approvisionnement en matières premières et services critiques. Elle vise aussi à permettre la divulgation sélective d'informations, garantissant ainsi que seules les données nécessaires sont partagées avec les parties concernées, tout en préservant la confidentialité et l'intégrité des informations sensibles.
Par exemple, un fournisseur pourrait prouver qu'un produit respecte certaines normes de qualité sans avoir à révéler les détails de ses processus de production et d'approvisionnement des services. Ce stage impliquera une analyse approfondie des besoins de sécurité des données dans différents cas d'usage, le développement d'un prototype de solution adapté à ce contexte, et l'évaluation de son efficacité pour améliorer la sécurité des données tout en facilitant la collaboration et la transparence entre les intervenants. L'ultime ambition est de poser les bases d'un écosystème de supply chain plus résilient et sécurisé, propice à l'innovation et à l'efficacité opérationnelle.

Le/La candidat(e) retenu(e) rejoindra le Laboratoire Systèmes d'Information de Confiance, Intelligents et Auto-Organisants (LICIA) au CEA LIST.

Méthodologie :
Le/La stagiaire aura les responsabilités suivantes :

1) **État de l'art et analyse des besoins** : Réaliser une revue exhaustive de la littérature et des solutions existantes autour de différentes techniques cryptographiques et des pratiques de sécurité des données dans la supply chain. Identifier les défis spécifiques liés à la sécurisation des échanges de données entre les acteurs de la supply chain et définir les besoins précis en termes de confidentialité et de sécurité des données.
2) **Conception de l'architecture de solution** : Élaborer une architecture détaillée pour la solution de partage de donnés en tenant compte des contraintes techniques et opérationnelles identifiées.
3) **Conception de l'architecture de solution** : Élaborer une architecture détaillée pour la solution de partage de donnés en tenant compte des contraintes techniques et opérationnelles identifiées.
4) **Développement du prototype** : Sur la base de l'architecture conçue, développer un prototype fonctionnel de la solution.
5) **Tests et validation** : Effectuer une série de tests pour valider la fiabilité, la sécurité, et la performance de la solution.
6) **Documentation et transfert de connaissances** : Rédiger une documentation complète de la solution.

Compétences :
Le/La candidat(e) doit avoir les compétences suivantes :

- Étudiant(e) master 2 en informatique/ingénierie.
- Connaissance en cryptographie, sécurité informatique.
- Connaissance de l'ingénierie du logiciel (expérience préalable des modèles de développement, du cycle de vie du logiciel, ou de l'intégration continue est un atout).

Domaine de spécialité requis : Informatique

Autres domaines de spécialités, mots clés :cryptographie, sécurité, blockchain, systèmes distribués, conception du logiciel, ingénierie du logiciel

Moyens mis en œuvre (expériences, méthodes d'analyses, autres...) :recherche, programmation

Niveau souhaité : Bac + 5 - Master 2

Durée : 6 mois

Niveau d'habilitation défense (AS au minimum):AS

Formation souhaitée : Ingénieur/Master

Possibilité de poursuit en thèse : Oui

Lieu du stage : CEA, Centre de Saclay Nano-Innov, 91191 Gif sur Yvette

Contacts :
MHADHBI Skander : skander.mhadhbi@cea.fr
ABDALLAH Rouwaida : rouwaida.abdallah@cea.fr
GARCIA PEREZ Alvaro : alvaro.garciaperez@cea.fr