RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Inserm
La science pour la santé
From science to health

HR EXCELLENCE IN RESEARCH

Chef de projet ou expert en ingénierie des systèmes d'information (F/H)

Concours externes 2024 – Ingénieurs et techniciens - Profil de poste – 1 poste

Emploi-Type	Chef de projet ou expert en ingénierie des systèmes d'information
Corps	IR - Ingénieur de recherche
BAP	E – Informatique, Statistiques et Calcul scientifique
Spécialité	Sécurité informatique / traitement de l'information
RIFSEEP (régime indemnitaire fonctionnaire)	Fonction : Ingénieur informatique Groupe : 2 Domaine : laboratoire
Affectation	**Unité 1101 - Laboratoire de traitement de l'information médicale (LATIM), BREST**
A propos de la Structure	Le LaTIM développe des technologies et des solutions innovantes afin d'améliorer le service médical rendu par l'intégration continue d'information multimodale, par nature hétérogène et complexe. Ces dernières années la science des données occupe une place prépondérante dans les activités des équipes du laboratoire. A l'heure de l'open data et de l'arrivée en force de l'intelligence artificielle (IA) dans le domaine de la santé, les enjeux de sécurité constituent un verrou majeur. Pour répondre à ces besoins, l'équipe Cyber Health du LaTIM, nouvellement créée, développe des solutions de tatouage, de crypto-tatouage et de traitements sécurisés. Le LaTIM a par ailleurs dans le domaine de cybersécurité des solutions et un savoir-faire méthodologique pour tatouer des données/des modèles d'IA chiffrées ou non, et traiter de manière sécurisée des données externalisées sur la base de techniques de chiffrement (homomorphe et autres), et de calcul multipartite sécurisé. Aujourd'hui, le LaTIM est impliqué dans différents projets collaboratifs où il a la charge de la protection des données et la sécurisation de traitements. Dans le cadre de projets tournés vers le « Big Health Data » (PEPR Santé Numérique, Hugoshare …), ses activités portent sur la traçabilité, la responsabilisation, la dissuasion et la lutte contre la fuite de données. Récemment, il s'intéresse à la sécurité des données stockées sur molécules d'ADN (PEPR MoleculArXiv). Au sein de la chaire industrielle CYBAILE et du projet Européen Horizon RIA PAROMA-MED, le LaTIM sécurise des traitements pour développer une IA de confiance en santé, dans un contexte fédéré ou centralisé. Ces aspects sont aussi étudiés/traités au travers du projet Labex CominLabs TADOP où, en collaboration avec l'UMR 1078, le LaTIM travaille sur la protection de données génétiques exploitées dans le cadre d'études d'association pangénomique. Il s'intéresse également à la sécurité des implants connectés (projet RHU Followknee). Ces solutions doivent profiter aux plateformes portées par l'INSERM.
Missions	Dans le cadre de projets allant du big health data à la sécurité de prothèses connectées, en passant par la génétique et l'imagerie médicale, la personne recrutée participera activement à l'élaboration et au déploiement d'outils permettant une protection continue des données de leur

	acquisition à leur réutilisation, et à la sécurisation de traitements de données externalisés (e.g. apprentissage fédéré). Il/Elle définira les plans d'études pour concevoir, adapter et intégrer les différentes méthodes et solutions de sécurité du LaTIM (tatouage, crypto-tatouage, partage sécurisé, machine Learning sécurisé, sécurité des données sur molécules d'ADN, …) et développera les outils informatiques afférents. Elle/Il interagira avec la DSI de l'Inserm pour intégrer ces solutions dans ses plateformes. Il/Elle diffusera et valorisera ces résultats auprès de la communauté scientifique française.
Activités principales	• Développer les plans d'études les mieux adaptés pour intégrer des outils de tatouage et de crypto-tatouage afin de répondre aux enjeux de sécurité de plateformes de collectes et de mises à disposition de données de santé • Proposer des solutions de traitements sécurisés de données sécurisées, notamment d'intelligence artificielle ou statistique dans un environnement fédéré, sur la base de techniques de tatouage, de crypto-tatouage, d'IA, de calcul multipartite sécurisé, de techniques cryptographiques • Identifier les enjeux de sécurité pour ces plateformes ouvertes par le biais d'analyse de risques en collaboration avec des partenaires (juriste, Data-Protection-Officer, administrateur système, Responsable Sécurité du Systèmes d'Information …) • Conseiller les membres de l'équipe dans la mise en œuvre de leurs traitements sur des données de santé, et les former sur l'utilisation des outils de sécurité développés • Diffuser et valoriser les résultats sous forme de publications et présentations orales dans des conférences • Co-encadrer des étudiants • Assurer une veille scientifique et technologique • Appliquer et faire appliquer les règles de bonnes pratiques en sécurité informatique.
Activités associées	• Animer des réseaux professionnels et permettre l'échange de connaissances.
Connaissances	• Connaissances en sécurité numérique • Connaissances approfondies en tatouage et crypto-tatouage de données et de modèles d'IA. • Connaissances en intelligence artificielle • Gestion du traitement de données massives (Spark, Hadoop, HDFS). • Connaissances en cryptographie • Connaissances en systèmes d'information et en bases de données : environnements Windows, Unix et Linux • Connaissances en développement informatique : C/C++, PYTHON - NumPy/SciPy, PyTorch, Git, Github … • Langue anglaise pour les présentations scientifiques et l'écriture d'articles (Overleaf, Latex)
Savoir-faire	• Expérience en tatouage et crypto-tatouage de données (bases de données, images) et/ou de protection de modèles d'IA. • Expérience en Machine Learning (méthodes d'apprentissage profond, apprentissage fédéré, NLP, reinforcement Learning, computer Vision, …). • Identification des besoins en sécurité des données de santé • Savoir identifier des workflows de données et les activités métier pour mener une analyse de risques et définir des exigences de sécurité • Développement logiciel.
Aptitudes	• Excellent relationnel/capacité d'intégration à des équipes de recherche pluri- et interdisciplinaire • Autonomie, sens de l'organisation, capacité d'analyse/d'écoute, sens critique • Confidentialité.

Spécificité(s) et environnement du poste	**Spécificités du poste** • Travail sur des données de santé, respect du cadre légal et déontologique • Activité hautement pluridisciplinaire requérant disponibilité, ouverture d'esprit et travail en équipe, en interne et en externe, intégrant ingénieurs, chercheurs et praticiens hospitaliers. • Données massives et traitements de données à protéger et sécuriser. **Environnement** • L' activité de cybersécurité concerne actuellement 3 chercheurs, 2 Ingénieurs de recherche, 3 Post-Doctorants, 8 Doctorants. • Bureau de deux personnes. • Laboratoire accessible en transport en commun.
Expérience souhaitée	• Expérience en protection des données et de modèles d'IA.
Diplôme(s) souhaité(s)	• Doctorat ou diplôme d'ingénieur.
Diplôme requis	• Niveau minimum de diplôme 7 (anciennement I).

Environnement de travail

Temps de travail	• Temps plein • Nombre d'heures hebdomadaires : 38h et 30mn • Congés Annuels et RTT : 32 jours ouvrés et 13 jours de RTT
Activités télétravaillables	☒ OUI * ☐ NON * A discuter avec le responsable hiérarchique
Rémunération	Selon la grille indiciaire correspondant au corps de recrutement, une reprise d'ancienneté selon le niveau d'expérience et un régime indemnitaire (RIFSEEP) correspondant à la fonction occupée. **Rémunération indicative brute moyenne mensuelle inclus IFSE*** (sur la base d'un indice moyen de rémunération) **: 3 203 €** ** Indemnité de Fonctions, de Sujétions et d'Expertise*
Pour en savoir +	• Sur l'Inserm : **https://www.inserm.fr/** ; site RH : **https://rh.inserm.fr/Pages/default.aspx** • Sur la politique handicap de l'Inserm et sur la mise en place d'aménagements de poste de travail, contactez la Mission Handicap : **emploi.handicap@inserm.fr** • Sur l'unité : https://nouveau.univ-brest.fr/latim/fr