Maitre.sse de conférences en « Sécurité Informatique»

Etablissement **:** ***Conservatoire national des arts et métiers***	Poste n° **: Galaxie 4310**

Corps :	MCF	**Article de référence** : 26-1
Section CNU :	**27 (Informatique)**	
Localisation : (Nom et adresse du site principal)	Conservatoire national des arts et métiers 292 rue Saint Martin, Paris 75141 Cédex 03	
Etat du poste :	Vacant	
Date prise de poste :	1er septembre 2024	

Le Conservatoire national des arts et métiers (Cnam) est un établissement public à caractère scientifique, culturel et professionnel doté d'un statut de « grand établissement » régi par le décret du 22 avril 1988. C'est un établissement en réseau dont le siège est à Paris qui se caractérise par :

- des formations déployées sur l'ensemble des régions métropolitaines, dans les centres ultra-marins et à l'étranger,
- des activités de recherche académique , technologique et partenariale au sein d'équipes reconnues par le HCERES,
- sa mission de diffusion de la culture scientifique et technique (notamment via le musée des arts et métiers).

La diversité et la richesse des équipes du Cnam dotent l'établissement d'un large spectre de compétences, couvrant les champs professionnels allant des sciences de l'ingénieur aux domaines de l'économie, de la gestion et des sciences humaines et sociales.

Les missions spécifiques dévolues aux enseignants-chercheurs du Cnam sont les suivantes :

- **Elaboration et mise en œuvre d'enseignements**
  - conception et animation d'enseignements sur l'ensemble des territoires,
  - actualisation des enseignements pour prendre en compte les besoins exprimés par les publics de la formation professionnelle et des territoires,
  - participation à la coordination des équipes pédagogiques et au suivi du déploiement de l'offre de formation, au bon déroulement et à la qualité des enseignements,
  - mise en place d'une offre de formation innovante (dont la formation à distance)
  - évaluation des acquis de l'apprentissage, participation aux jurys.

- **Développement des activités de recherche et/ou d'innovation**
  - développement de projets de recherche académique ou partenariale à l'échelle nationale, européenne et internationale,
  - formation par et à la recherche,
  - valorisation des travaux de recherche,
  - développement de liens et de coopérations avec des chercheurs français et étrangers et les milieux professionnels concernés.

- **Diffusion de la culture scientifique et technique**
  - Diffusion de pratiques pédagogiques,
  - Communication scientifique et technique vers la société (organisation de congrès, conférences grand public…).

- **Participation à la vie de l'établissement et à sa promotion**

Profil

Profil enseignement :	Les missions envisagées pour le.a MCF au sein de l'EPN 05 : - dispenser une unité d'enseignement sur la cybersécurité des infrastructures informatiques (niveau I2 ou I3 du diplôme d'ingénieur en informatique) : le candidat devra proposer un projet d'intégration dans deux unités d'enseignements du diplôme, majeure cybersécurité ; - participer aux enseignements de niveau M1 et M2 dispensés dans le cadre du Master Sécurité Informatique, Cybersécurité et Cybermenaces : le candidat devra proposer un projet d'intégration dans deux unités du master ; - participer ou prendre en charge le pilotage de la future plateforme Cnam cyber en lien avec ces enseignements, - participer aux tutorats de mémoire d'ingénieur et de master.
Job profile : *brève synthèse de quatre lignes en anglais comprenant les coordonnées de la composante qui publie le poste, le profil du poste (2 lignes max.) et le contact pour envoi de la candidature avec la date limite.*	The associate-professor position offered by CNAM computer science department, EPN05, is open to teach cybersecurity, network/IoT security and data security. Teachings cover graduate modules (BAC+3 to BAC+5 classes) : two daytime modules, and one evening/remote teaching classes, and sandwich courses.
EPN :	EPN 05 - Informatique
Mots-clés enseignement :	Sécurité des infrastructures Cloud, IoT, réseau. Blockchain. Analyse de codes malveillants. Sécurité des données. Sécurité des architectures matérielles.

Profil recherche :	Le.la candidat.e intégrera l'équipe ISID ou l'équipe ROC de l'axe 3 (confiance et sécurité numériques) du laboratoire CEDRIC (https://cedric.cnam.fr). Son activité de recherche s'inscrira dans le cadre des travaux de recherche de cybersécurité menés au sein de ces deux équipes. Le.la candidat.e intégrera les projets de recherche en cours et à venir, menés également en collaboration avec d'autres laboratoires ou équipes du Cnam. Au sein de l'équipe ISID, un projet d'équipe transverse portant sur la cybersécurité des infrastructures critiques, en particulier les systèmes industriels, offrira des axes de développement pour la recherche du.de la candidat.e. L'équipe ISID développe plusieurs travaux de recherche en sécurité informatique qui pourraient accueillir le.la candidat.e : les thématiques portent sur la génération automatique de modèles d'explication et de chemins d'attaques, à base d'IA ("knowledge graph", "treillis", "ontologies") /ML pour modéliser puis explorer les données d'incident (logs, OSINT,...), pour l'analyse de vulnérabilités (MITRE TTP), la détection d'anomalie, l'investigation numérique et l'analyse de risque. Les projets en cours sont 1 ANR (CoRReAU) obtenu en 2022, et des contrats industriels signés en 2022/2023. Au sein de ces projets, le.la candidat.e. pourra également développer des travaux sur l'évaluation de la sécurité : IoC (indicateurs de compromission), évaluation de graphes d'attaques, de politiques de sécurité, de codes malveillants dans les binaires. Les cas d'applications cyber sont les véhicules connectés, la santé, les drones, les réseaux d'eau (CPS/PLC/SCADA), les IIoT, etc. Au sein de l'équipe ROC, les activités du.de la candidat.e porteront sur la sécurité des systèmes embarqués, sur la définition et l'évaluation d'algorithmes de détection d'attaques, sur la fiabilité des réseaux et des systèmes distribués, et sur la protection des données personnelles (dans un contexte IoT en combinant des mécanismes de chiffrement et d'anonymisation). De plus, le.la candidate est susceptible de travailler sur la gestion auto-souveraine des identités numériques en utilisant la Blockchain, la gestion de pannes d'infrastructure, la détection d'intrusions et de chemins d'attaques dans les systèmes cyber-physiques en explorant des méthodes d'IA (comme les GNN). Les derniers projets qui portent

	sur ces thèmes sont : leprojet H2020 « A Secure and Reusable Artificial Intelligence Platform for Edge Computing in Beyond 5G Networks (AI@EDGE) », len projet ANR GNADiS qui a démarré en octobre 2023 et le projet européen GRAPH4SEC sur la détection d'attaques et de pannes à l'aide des GNN. L'équipe a de plus des contrats bilatéraux avec Thales sur chiffrement et détection d'attaques, avec Sopra Steria sur les Blockchains, avec Orange sur les modèles de sécurité pour les systèmes embarqués, et avec CS Covidy's sur les GNN. Plusieurs thèses en cours forment un terrain fertile de départ pour ces travaux : utilisation des modèles d'IA sur des données chiffrées homomorphiquement, protection des données IoT à l'aide de la confidentialité différentielle et de l'apprentissage fédéré, gestion souveraine des identités numériques à l'aide de la technologie Blockchain, sécurité des VANETs, détection d'anomalies à l'aide de techniques d'IA/ML, etc. Les activités de recherche de.la candidat.e doivent porter sur les thèmes d'une des équipes ou sur les deux. Le.la candidat.e pourra ainsi développer l'activité de recherche autour des plateformes d'entrainement et d'expérimentation existantes et à venir, et encadrer les travaux scientifiques associés, par exemple par l'encadrement de doctorants et d'étudiants des masters orientés recherche. Un bon équilibre entre les différentes activités (enseignement, recherche et administration) sera particulièrement apprécié.
Job profile : *brève synthèse de deux lignes en anglais du profil du poste.*	The hired associate-professor will do his/her research activities with ROC or ISID team of CEDRIC Lab on cybersecurity, network/IoT security, information system security and data protection.
Laboratoire : *(nom + n°)*	**CEDRIC (EA 4629)**
Mots-clés recherche :	Sécurité des systèmes embarqués/IoT et des réseaux, détection d'anomalies, analyse de vulnérabilités, protection des données personnelles.

Informations complémentaires :

Enseignements :	
Equipe :	EPN05 – Informatique https://deptinfo.cnam.fr
Lieux d'exercice :	Cnam, Paris
Nom du directeur de l'équipe :	Stefano Secci
Téléphone de la directrice de ou du directeur de l'équipe :	(mail préférable)
Email de la directrice ou du directeur de l'équipe :	Stefano.secci@cnam.fr

Recherche :	
Lieux d'exercice :	Cnam, 2 rue conté, 75003 Paris
Nom de la directrice ou du directeur du laboratoire :	Samia Bouzefrane
Téléphone de directrice ou du directeur du laboratoire:	(mail préférable)
Email de directrice du laboratoire :	samia.bouzefrane@cnam.fr
URL du laboratoire :	https://cedric.cnam.fr
Descriptif du laboratoire :	Fondé en 1988, le Cédric regroupe l'ensemble des activités de recherche en informatique, mathématiques appliquées et électronique menées au Cnam. A l'exception de quelques extérieurs, les membres du Cédric sont des enseignants-chercheurs du CNAM en Informatique, en Mathématiques Appliquées ou en Electronique. Les recherches du laboratoire couvrent un large domaine et sont développées autour de 8 axes :

	- Bases de Données Avancées (Vertigo) - Ingénierie des Systèmes d'Information et de Décision (ISID) - Interaction pour Lire et Jouer (ILJ) - Méthodes Statistiques de Data Mining et Apprentissage (MSDMA) - Systèmes Sûrs (Sys) - Réseaux et Objets Connectés (ROC) - Optimisation Combinatoire (OC) - Radiocommunications (Laetitia)
Lien pour le rapport du HCERES du laboratoire :	http://cedric.cnam.fr/HCERES/

Composition du comité de sélection

Membres appartenant à l'établissement : 7				
Nom et prénom	Qualité	Homme/ Femme	Section CNU	Discipline enseignée ou de recherche
Samira Cherfi	PU	F	27	Informatique - Systèmes d'information
Cédric du Mouza	PU	H	27	Informatique - Systèmes d'information & BDD
Pierre Paradinas	PRCM	H	27	Informatique – Sécurité des systèmes embarqués
Maria-Virginia Aponte	MCF	F	27	Informatique - Systèmes sûrs
Faten Atigui	MCF	F	27	Informatique - Systèmes d'information & BI
Stéphane Rovedakis	MCF	H	27	Informatique - Systèmes distribués
Tatiana Aubonnet	MCF	F	27	Informatique – Internet des objets

Membres extérieurs à l'établissement : 7					
Nom et prénom	Qualité	Homme/ Femme	Section CNU	Discipline enseignée ou de recherche	Etablissement d'affectation
Geraldine Texier	PU assimilée	F	27	Informatique - Sécurité des réseaux	IMT Atlantique
Mohand Said Hacid	PU	H	27	Informatique - Sécurité des systèmes d'informations	Université Claude Bernard Lyon 1
Hakima Chaouchi	PU	F	27	Informatique – sécurité des réseaux/Cloud/IoT-privacy	Télécom SudParis, Institut Polytechnique de Paris
Vincent Nicomette	PU	H	27	Informatique – sécurité IoT	INSA de Toulouse
Samiha Ayed	MCF	F	27	Informatique - Sécurité des systèmes d'informations	Université de Technologie de Troyes (0101060Y)
Johanne Vincent	MCF assimilée	F	27	Informatique – cybersécurité – gestion d'identités	IMT Atlantique
Martino Borello	MCF	H	26	Sécurité et Cryptographie	Université Sorbonne Paris Nord

- **<u>Présidente du comité de sélection</u>** Madame Hakima Chaouchi professeure des universités à Télécom SudParis, Institut Polytechnique de Paris

- **<u>Vice-président du comité de sélection</u>** Monsieur Pierre Paradinas, professeur du Conservatoire national des arts et métiers