**Titre de la thèse/Thesis title :** Détection d'anomalies frugale, distribuée et explicable dans les réseaux d'objets connectés sans fil à perception visuelle

**Laboratoire d'accueil / Host Laboratory :** ImViA UR 7535

**Spécialité du doctorat préparé/Speciality :** Informatique

**Mots-clefs / Keywords :** Détection d'anomalies, Edge AI, Cybersécurité, IoT, Réseaux de capteurs visuels intelligents, Modèles d'apprentissage légers et distribués.

**Descriptif détaillé de la thèse / Job description**

## 1. Contexte scientifique

Les réseaux d'objets connectés sans fil constituent aujourd'hui une infrastructure essentielle pour de nombreuses applications critiques, allant de la surveillance environnementale aux systèmes de sécurité intelligents. Ces réseaux reposent sur des dispositifs hétérogènes, interconnectés via des technologies de communication à faible consommation, et opérant dans des environnements fortement contraints. L'intégration croissante de capteurs visuels intelligents (notamment des caméras embarquées) capables de produire des flux riches et complexes constitue une évolution de ces réseaux. Toutefois, ces dispositifs demeurent fortement limités en ressources (capacité de calcul limitée, mémoire restreinte, autonomie énergétique réduite et connectivité intermittente), ce qui impose de repenser en profondeur les méthodes de traitement et d'analyse des données.

Dans ces environnements distribués, dynamiques et contraints, la détection d'anomalies constitue un enjeu fondamental pour assurer la fiabilité, la sécurité et la résilience des systèmes [1]. Ces anomalies peuvent être d'origine multiple : défaillances matérielles, perturbations environnementales, erreurs de configuration, ou attaques malveillantes (injection de données, compromission de nœuds, attaques adversariales sur les flux visuels). Les fortes contraintes en ressources rendent difficile l'adoption d'approches classiques de détection d'anomalies, souvent fondées sur des modèles d'apprentissage profond centralisés et coûteux [2]. Ces limitations sont encore plus marquées dans le cas des capteurs visuels, où le traitement des données (images ou vidéos) est intrinsèquement plus exigeant.

## 2. Problématique scientifique

Comment concevoir des mécanismes de détection d'anomalies capables d'opérer de manière distribuée, frugale et explicable au sein de réseaux d'objets connectés sans fil intégrant des capteurs visuels contraints, tout en garantissant un compromis optimal (ou presque) entre précision de détection, consommation de ressources et robustesse face à des environnements dynamiques et potentiellement adversariaux ? Cette problématique se situe au croisement de l'apprentissage automatique embarqué, des systèmes distribués et de la cybersécurité.

Dans ce contexte, les paradigmes d'*Edge AI* [3, 4] et d'apprentissage frugal apparaissent comme des solutions particulièrement prometteuses, en permettant de rapprocher les capacités d'analyse des sources de données, de réduire la latence décisionnelle et de limiter les échanges réseau. Toutefois, la conception de modèles à la fois légers, précis, robustes et économes en ressources pour la détection d'anomalies dans ces réseaux constitue un défi scientifique majeur. Une attention particulière sera portée aux approches fondées sur la *distillation de connaissances* [5], permettant de transférer les performances de modèles complexes vers des architectures plus compactes, adaptées à une exécution embarquée.

## 3. Verrous scientifiques

Plusieurs verrous scientifiques majeurs doivent être levés. Le premier concerne la conception de modèles d'intelligence artificielle frugaux. Il s'agit de développer des approches capables de traiter efficacement des données complexes sur des dispositifs fortement contraints en ressources. Les techniques de distillation de connaissances, de compression, de quantification ou encore de conception d'architectures légères doivent être repensées afin de garantir un compromis optimal entre compacité, précision et capacité de généralisation, dans des environnements dynamiques.

Le deuxième verrou réside dans la détection distribuée et collaborative des anomalies. L'absence de centralisation des données et les contraintes de communication imposent de concevoir des mécanismes capables d'exploiter l'intelligence collective du réseau. Cela soulève des questions fondamentales relatives à la coordination entre nœuds, à la fusion d'informations hétérogènes, ainsi qu'à la gestion des compromis entre détection locale et globale, dans des contextes de connectivité intermittente. Il convient également de proposer des stratégies d'optimisation conjointe visant à réduire la consommation énergétique et la charge de communication induites par les mécanismes de détection.

Un troisième verrou majeur concerne la robustesse des modèles face aux menaces adversariales. Cela implique le développement de mécanismes d'adaptation continue et de défense intégrée.

Enfin, un dernier verrou porte sur l'explicabilité des décisions dans des environnements contraints.

**Références bibliographiques / Bibliography**

[1] Abba Ari, A. A., Samafou, F., Ndam Njoya, A., Djedouboum, A. C., Aboubakar, M., & Mohamadou, A. (2025). *IoT-5G and B5G/6G resource allocation and network slicing orchestration using learning algorithms*. IET Networks, 14(1), e70002.

[2] Wang, X., Tang, Z., Guo, J., Meng, T., Wang, C., Wang, T., & Jia, W. (2025). *Empowering edge intelligence: A comprehensive survey on on-device ai models*. ACM Computing Surveys, 57(9), 1-39.

[3] Gauttam, H., Nain, G., Pattanaik, K.K., Mendes, P. (2026). *Edge-AI: A systematic review on architectures, applications, and challenges*. Journal of Network and Computer Applications, 245.

[4] Patrick, B., Kanjo, E., Kaiwartya, O. (2026). *Review of Movement Sensor Applications in Livestock Animal Activity Recognition: Communications, Data Collection Practices, and Edge-AI Solutions*. Smart Agricultural Technology.

[5] De Rose, L., Andresini, G., Appice, A., Malerba, D. (2026). *VINCENT: Cyber-threat detection through vision transformers and knowledge distillation*. Computers & Security.

**Profil demandé / Applicant profile**

Le candidat ou la candidate devra être titulaire d'un diplôme de niveau Master 2 (ou équivalent) en informatique ou un domaine assez proche, avec une spécialisation en intelligence artificielle, systèmes embarqués, réseaux ou cybersécurité. Une formation à l'interface de plusieurs de ces domaines sera particulièrement appréciée.
Il/elle devra posséder de solides compétences en apprentissage automatique (notamment deep learning) et en programmation (Python, PyTorch/TensorFlow). Une sensibilité aux environnements contraints (Edge AI), à la détection d'anomalies et au traitement de données visuelles constituera un atout. L'autonomie et l'aptitude à la rédaction en anglais sont indispensables.

**Financement : MESRI Etablissement**

Dossier à envoyer pour le 18 mai 2026

Début du contrat : 1er Octobre 2026
Salaire mensuel brut : 2300€

**Direction de la thèse:/ Thesis Supervisor**

ABDOU Wahabou : wahabou.abdou@ube.fr

**Encadrement de la thèse : co-directeur(s) et co-encadrant(s)**

DUBOIS Julien : julien.dubois@ube.fr (co-directeur)

Les dossiers de candidature, contenant les pièces suivantes, devront être envoyés par mail aux encadrants de la thèse :

- CV
- Lettre de motivation
- Relevé de notes du Master
- Eventuelles lettres de recommandation ou une liste de personnes de référence