



## AVIS DE SOUTENANCE D'UNE THESE DE DOCTORAT

Le Directeur de l'Ecole Nationale des Sciences Appliquées a le plaisir d'informer le public  
qu'une soutenance de thèse de Doctorat en

«**Sciences et ingénierie**»

aura lieu le 11/10/2025 à 10H à l'ENSA de Kénitra

La Thèse sera présentée par Mr KABLY SALAH-EDDINE

Sous le thème :

**AI-Enhanced Blockchain Architecture for Proactive Security Management in  
Resource-Limited IoT Networks**

Devant le jury composé de :

| Nom et Prénom      | Titre                    | Etablissement                         |
|--------------------|--------------------------|---------------------------------------|
| SRIFI NABIL        | Président                | ENSA, Kénitra                         |
| BOULMALF MOHAMMED  | Rapporteur               | Université Internationale de Rabat    |
| AZMANI MONIR       | Rapporteur               | Faculté Polydisciplinaire de Larache  |
| MOUMEN ANISS       | Rapporteur               | ENSA, Kénitra                         |
| EL HAMI NORELISLAM | Examineur                | ENSA, Kénitra                         |
| LAANAOUI MY DRISS  | Examineur                | Ecole Normale Supérieure de Marrakech |
| ALAOUI NABIH       | Co-Directeur de<br>thèse | Université Internationale de Rabat    |
| ARIOUA MOUNIR      | Directeur de thèse       | ENSA, Kénitra                         |





**Nom et Prénom : KABLY SALAH-EDDINE**

**Date de soutenance : 11/10/2025**

**Directeur de Thèse : ARIOUA MOUNIR**

**Sujet de thèse :**

## **AI-Enhanced Blockchain Architecture for Proactive Security Management in Resource-Limited IoT Networks**

**Résumé:**

L'intégration de la technologie blockchain et de l'Internet des Objets promet d'améliorer la sécurité et la confidentialité des objets connectés. Cependant, les ressources limitées de ces objets et les difficultés à adapter la blockchain à grande échelle constituent des obstacles importants. Cette thèse propose deux solutions pour surmonter ces défis. Premièrement, une architecture blockchain légère basée sur une structure de graphe acyclique dirigé est proposée. Elle utilise le fog computing pour décharger les tâches des objets connectés, améliorant ainsi l'efficacité énergétique et la réactivité. Cette architecture intègre une authentification forte, une structure multi-zones, l'algorithme Blowfish amélioré et un graphe acyclique dirigé bayésien, ainsi qu'un système combinant réseaux neuronaux à convolution profonde et réseaux antagonistes génératifs pour la détection d'intrusion. Deuxièmement, un système de détection et de prévention des intrusions basé sur une blockchain multi-zones est présenté. Il utilise l'algorithme Blowfish amélioré pour l'authentification, le graphe acyclique dirigé bayésien pour la gestion du réseau, et combine réseaux neuronaux à convolution profonde et réseaux antagonistes génératifs pour la classification des données. Une fonction de reconstruction de scénario d'intrusion est également implémentée. Des simulations sur des données réelles démontrent l'efficacité de ces solutions en termes d'économie d'énergie, de réduction de l'espace de stockage nécessaire, de rapidité de réponse et de taux de détection d'attaques. Ces travaux proposent des solutions blockchain légères et efficaces, adaptées aux contraintes de l'Internet des Objets, ouvrant la voie à des environnements d'objets connectés plus sûrs et plus fiables. Ils constituent une contribution significative à la sécurité de l'Internet des Objets. Mots Clés: Blockchain, IoT, Sécurité, Intrusion Detection, Fog Computing.

**Abstract:**

The convergence of blockchain and the Internet of Things (IoT) presents significant opportunities for bolstering the security and privacy of connected devices. Nevertheless, the resource constraints inherent in IoT devices and the scalability limitations of traditional blockchain architectures present substantial hurdles. This thesis puts forward two novel solutions to address these challenges. First, a lightweight blockchain architecture founded upon a directed acyclic graph structure is introduced. This architecture leverages fog computing to offload computational tasks from resource-constrained IoT devices, thereby enhancing energy efficiency and responsiveness. It incorporates robust authentication mechanisms, a multi-zone structural design, an enhanced Blowfish algorithm, and a Bayesian directed acyclic graph. Furthermore, it integrates a sophisticated intrusion detection system that synergistically combines deep convolutional neural networks and generative adversarial networks. Second, a multi-zone blockchain-based intrusion detection and prevention system is presented. This system employs the enhanced Blowfish algorithm for device authentication, the Bayesian directed acyclic graph for efficient network management, and a hybrid approach using deep convolutional neural networks and generative adversarial networks for accurate data packet classification. Additionally, it features an intrusion scenario reconstruction capability. Extensive simulations using real-world datasets demonstrate the efficacy of the proposed solutions in terms of energy conservation, storage overhead reduction, response latency, and attack detection accuracy. This research advances lightweight and efficient blockchain solutions tailored to the specific constraints of the IoT paradigm, paving the way for more secure and trustworthy connected environments. It represents a significant contribution to the burgeoning field of IoT security. Key words : Blockchain, IoT, Security, Intrusion Detection, Fog Computing.