Fiche de synthèse
Programme de cotutelle U. Sfax-UTT

Description du contexte de la thèse

Nom et prénom du porteur du projet : Ayed Samiha
Adresse mail : samiha.ayed@utt.fr
Fonction (PR, MCF…) : MCF- HDR
Date HDR du porteur : 14/03/2025
Établissement : Université de Technologie de Troyes Adresse web : https://www.utt.fr/
Laboratoire : LIST3N Adresse web : https://recherche.utt.fr/list3n
Compétence scientifique : cybersécurité, IA, IoT
Noms et prénoms des codirecteurs de la thèse : Samiha Ayed & Lamia Chaari Fourati
Deux publications en relation avec le sujet proposé :

1- Achref Haddaji, Samiha Ayed, Lamia Chaari Fourati, Artificial Intelligence techniques to mitigate cyber-attacks within vehicular networks: Survey, Computers and Electrical Engineering, Volume 104, Part B, 2022
2- Fadhila Tlili, Samiha Ayed, Lamia Chaari Fourati, Exhaustive distributed intrusion detection system for UAVs attacks detection and security enforcement (E-DIDS), Computers & Security, Volume 142, 2024

Description du sujet de thèse proposé

Titre : Approches hybrides basées sur l'IA pour la spécification et le déploiement des politiques de réaction dans l'IoT.
Mots-clés : Politiques de réaction ; IA ; Attaques ; Deep learning ; Apprentissage par renforcement ; IoT
Sujet : L'Internet des Objets (IoT) est un écosystème hétérogène exposé à de nombreuses cybermenaces, nécessitant des politiques de sécurité dynamiques et adaptatives. L'approche hybride combinant Deep Learning (DL) et Apprentissage par Renforcement (RL) offre une solution prometteuse pour spécifier et déployer ces politiques de manière autonome et efficace. Le DL permet d'analyser les flux de données en temps réel pour détecter les attaques connues et émergentes, tandis que le RL optimise les réponses et l'adaptation aux menaces évolutives. L'intégration de ces deux approches améliore la prise de décision et la résilience des systèmes IoT face aux cyberattaques. Ce sujet vise à explorer les architectures hybrides DL-RL, leur mise en œuvre dans des environnements IoT et leur efficacité par rapport aux méthodes classiques de cybersécurité.
Les différentes tâches sont comme suit :

1- Tâche 1 : Etat de l'art sur l'usage des approches hybrides pour gérer les politiques des réactions dans des environnements IoT.
2- Tâche 2 : Proposer une spécification formelle de politiques de réaction dynamiques et contextuelles.
3- Tâche 3 : Proposer des approches hybrides basées sur l'apprentissage profond et l'apprentissage par renforcement pour le déploiement de ces politiques de réaction.
4- Tâche 4 : Proposer une approche d'intégration en temps réel de ces approches de réaction dans un environnement IoT en utilisant un cadre applicatif spécifique.
5- Tâche 5 : Vérifier formellement de la proposition en utilisant un outil de spécification formelle (langage Z, modèle cheking, etc.).
6- Tâche 6 : Evaluation des résultats dans des environnements d'IoT.

Collaborations attendues :
Les deux co-directeurs de thèse ont des compétences complémentaires. Le membre de l'UR LIST3N apportera son expertise en cybersécurité et en usage des techniques de l'IA pour la sécurisation des scénarios. Le membre du laboratoire SM@RTS ramènera les compétences dans le domaine de l'IA et de la gestion des données. Les deux co-directeurs ont déjà collaboré ensemble et possèdent une liste pertinente de publications communes. Ce sujet aidera à renforcer cette collaboration et à étendre ses perspectives.

Compétences nécessaires du candidat :
Le candidat doit avoir une formation de niveau Bac + 5 en informatique (Master2 ou ingénieur) avec éventuellement une spécialisation en réseau ou en sécurité ou aussi en IA. Une connaissance du domaine de la cybersécurité et/ou en intelligence artificielle sera très appréciées.

Existence d'un fichier pdf détaillant le sujet : oui/~~non~~