Programme de cotutelles U. Sfax- UTT

Description du sujet (merci de vous conformer aux recommandations indiquées sur le site web)

Nom :	Ayed	Prénom :	Samiha
Fonction (prof., MdC) :	MdC		
Laboratoire :	LIST3N	Adresse web :	https://recherche.utt.fr/list3n
Etabliss[t] :	UTT	Adresse web :	https://www.utt.fr/

Compétence scientifique:

Samiha Ayed possède des compétences scientifiques en cybersécurité, plus spécifiquement en gestion de politiques de sécurité, détection d'intrusion, utilisation d'approches d'intelligence artificielle pour la détection d'attaques, validation formelle des propriétés de sécurité, traçabilité et privacy.

2 publications importantes en relation avec le sujet proposé :

- Achref Haddaji, Samiha Ayed, Lamia Chaari Fourati: A23Artificial Intelligence techniques to mitigate cyber-attacks within vehicular networks: Survey. Comput. Electr. Eng. 104(Part): 108460 (2022)
- Fadhila Tlili, Samiha Ayed, Lamia Chaari Fourati: A New Hybrid Adaptive Deep Learning-Based Framework for UAVs Faults and Attacks Detection. IEEE Trans. Serv. Comput. 16(6): 4128-4139 (2023)

Adresse web de votre page personnelle :

Adresse mail : samiha.ayed@utt.fr

Description du sujet de thèse proposé ***n° du thème :*** 2

Titre : Un framework sécurisé basé sur l'IAG (Intelligence Artificielle Générative)

Sujet :

Dans cette thèse, nous nous focalisons sur le lien entre les attaques adverses et les modèles de l'intelligence artificielle générative. Nous proposerons des modèles génératifs pour détecter des schémas de comportement suspects ou pour générer des données de test plus réalistes afin d'évaluer la résilience des systèmes de sécurité. Pour la mise en pratique des solutions qui seront proposées, nous utiliserons les modèles d'IAG pour générer des données d'entraînement supplémentaires afin d'améliorer les modèles de détection des menaces. Cela peut aider à renforcer la robustesse des systèmes de cybersécurité en exposant les modèles à un large éventail de scénarios possibles. Les étapes de cette thèse sont comme suit :

1- Une étude approfondie de l'état de l'art sur les techniques d'attaques qui se basent sur l'IAG.
2- La proposition d'une taxonomie pour les différents modèles basés sur l'IAG pour contrer les cyber-attaques basés sur des modèles génératifs.
3- Proposition d'un modèle basé sur l'IAG qui permet de détecter et de réagir aux attaques adverses.
4- Proposition d'un méta-modèle générique en se basant sur une classification définie pour les attaques génératives.
5- Validation du modèle proposé avec des use-cases et de différents scénarios réels.

mots clés :

IA, modèles de sécurité, attaques

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) : Oui

(respecter les indications données sur le site web)