Avis de Soutenance

Monsieur Song SHOMBOT

Soutiendra publiquement ses travaux de thèse intitulés

UNE APPROCHE DE CYBERSÉCURITÉ À PLUSIEURS NIVEAUX POUR LE SECTEUR DES SOINS DE SANTÉ BASÉE SUR LA TECHNOLOGIE DES BASES DE DONNÉES, L'INTELLIGENCE ARTIFICIELLE ET L'ÉVALUATION DES RISQUES

dirigés par Monsieur Gilles DUSSERRE et Robert BESTAK

Soutenance prévue le ***mardi 25 mars 2025*** à 14h00
Lieu : Univeristé de Nimes - Site Vauban 5 Rue du Docteur Georges Salan CS 13019 30021 Nîmes
Salle : du Conseil

Composition du jury proposé

M. Gilles DUSSERRE	Nîmes Université	Directeur de thèse
M. Gouenou COATRIEUX	IMT Atlantique	Rapporteur
M. Didier VAN CAILLIE	Université de Liège	Rapporteur
M. Robert BESTAK	CTU Prague	Co-directeur de thèse
M. Stéphane LECOEUCHE	IMT Mines Alès	Co-encadrant de thèse
M. Jean-Yves LEFRANT	CHU Nîmes	Examinateur

Mots-clés : Cybersécurité,Technologie des bases de données,Détection des intrusions,Intelligence artificielle (IA),Apprentissage machine (ML),Évaluation des risques

Résumé :

Ces dernières années, les cyberattaques sont devenues de plus en plus fréquentes et sophistiquées, faisant de la cybersécurité dans le secteur des soins de santé une préoccupation mondiale urgente. Parmi les facteurs responsables de cette fragilité, on peut citer la dépendance excessive des établissements de santé à l'égard des infrastructures numériques reliées, les informations sensibles sur les patients et l'utilisation de systèmes de sécurité obsolètes. Cette thèse explore une approche multicouche de la cybersécurité dans les soins de santé en utilisant la technologie des bases de données, l'intelligence artificielle (IA), l'apprentissage machine (ML) et les méthodologies d'évaluation des risques. Nous commençons par évaluer le paysage actuel des menaces au moyen d'une application web qui exploite les enregistrements de cyberincidents accessibles au public, principalement du Center for International and Security Studies Maryland (CISSM), qui contient plus de 1 500 cas liés aux soins de santé, et de l'Office for Civil Rights (OCR), qui a documenté plus de 800 incidents ayant fait l'objet d'une enquête. La plateforme développée permet aux utilisateurs d'ajouter, de supprimer, de rechercher, de visualiser et de télécharger des incidents cybernétiques. Pour traiter les vulnérabilités en matière de cybersécurité, nous présentons le cadre d'évaluation des risques cybernétiques de l'hôpital universitaire de Baze (BUHCRAF), appliqué à l'hôpital universitaire de Baze en tant qu'étude de cas. Ce cadre identifie plus de 50 risques de sécurité, dont certains

sont liés à des menaces connues documentées dans la base de données Common Vulnerabilities and Exposures (CVE). Les principaux risques comprennent les logiciels non corrigés, les dispositifs médicaux IoT non sécurisés et les contrôles d'accès faibles. Sur la base de ces connaissances, des solutions de cybersécurité pilotées par l'IA/ML sont proposées. L'étude comprend plusieurs études de cas démontrant les applications de l'IA/ML dans la cybersécurité. Le premier cas porte sur la détection d'anomalies dans l'Internet de la santé des objets (IoHT), en utilisant l'ensemble de données ECU-IoHT contenant 111 000 enregistrements et cinq classes d'attaques (Normal, Nmap, DoS, ARP, Smurf). Nous comparons quatre modèles ML - Forêt aléatoire (RF), Gradient Boosting (GB), Arbres de décision (DT) et Perceptron multicouche (MLP) - où GB atteint la plus grande précision de 99,53%. La deuxième étude de cas applique l'IA/ML à la détection du phishing, en analysant des caractéristiques telles que l'URL de la requête, l'âge du domaine, le statut HTTPS/SSL, le trafic du site web et les pop-ups. Des machines à vecteurs de support (SVM) ont été utilisées avec deux fonctions de noyau : la fonction de base radiale (RBF) et la fonction polynomiale. Le noyau polynomial est plus performant que le noyau RBF, avec une précision de 84,5 % contre 82,6 %. La troisième étude de cas explore l'IA/ML dans la détection des intrusions en proposant un cadre Cross-ML utilisant trois ensembles de données publiques : UNSW-NB15, X-IIoTID et ToN-IoT. Les modèles individuels impliquent des modèles formés sur leurs ensembles de données respectifs qui ont obtenu des scores F1 allant de 92,0 % à 98,1 %, tandis que l'approche combinée des ensembles de données a enregistré une précision de 90,9 %, un rappel de 84,0 % et un score F1 de 84,9 %. Les évaluations transversales ont montré que le modèle X-IIoTID testé sur ToN-IoT a obtenu les meilleures performances, avec une précision de 75 % et un score F1 de 74 %. Cette recherche souligne l'importance d'une approche de cybersécurité multicouche qui intègre une approche axée sur les bases de données, des applications de sécurité améliorées par l'IA/ML et des cadres d'évaluation des risques structurés pour renforcer la résilience de la cybersécurité dans les organismes de soins de santé.