Avis de Soutenance

Monsieur USMAN RABIU ISAH

Informatique

Soutiendra publiquement ses travaux de thèse intitulés
Cybersécurité assistée par l'IA pour l'agriculture 4.0

Travaux dirigés par Monsieur Pascal BERTHOMÉ

Ecole doctorale : Mathématiques, Informatique, Physique Théorique et Ingénierie des Systèmes - MIPTIS
Unité de recherche : LIFO - Laboratoire d'Informatique Fondamentale d'Orléans

Soutenance prévue le ***lundi 11 mai 2026*** à 14h00
Lieu : INSA Centre Val de Loire, 88 Boulevard Lahitolle, 18000 Bourges, France
Salle : Amphithéâtre Sapphira

Composition du jury proposé

M. Pascal BERTHOMÉ	Professeur des universités	INSA Centre Val de Loire	Directeur de thèse
M. Philippe OWEZARSKI	Directeur de recherche	LAAS-CNRS	Rapporteur
M. Jean-François LALANDE	Professeur des universités	CentraleSupélec	Rapporteur
M. Laurent BOBELIN	Enseignant-Chercheur Contractuel	INSA Centre Val de Loire	Co-encadrant de thèse
M. Adel HAFIANE	Professeur des universités	Université d'Orléans	Examinateur
M. Gil UTARD	Professeur des universités	Université Picardie Jules Verne	Examinateur
Mme Clara BERTOLISSI	Professeure des universités	INSA Centre Val de Loire	Examinatrice
Mme Nancy AWAD	Maître de conférences	Université Marie et Louis Pasteur	Examinatrice

Mots-clés : Intelligence artificielle, Apprentissage fédéré, Systèmes de détection d'intrusion, Attribution d'Auteur, Agriculture 4.0, Cybersécurité

Résumé :

Le secteur agricole connaît une transformation numérique rapide vers l'Agriculture 4.0, caractérisée par l'intégration d'objets connectés (IoT), de l'intelligence artificielle et de machines autonomes. Cette évolution a donné naissance à un écosystème complexe et multi-fournisseurs, de plus en plus vulnérable aux cybermenaces. Cette thèse examine l'efficacité des systèmes de détection d'intrusion (IDS) au sein de cet environnement hétérogène et aux ressources limitées. La recherche identifie d'abord les défis opérationnels liés au déploiement des IDS dans l'agriculture connectée, notamment des risques spécifiques tels que les vulnérabilités liées à l'enregistrement à distance des données et la gestion de la sécurité des équipements existants (« brownfield »). Pour pallier les limites de la défense collaborative, l'étude quantifie les risques pour la vie privée liés au partage de règles de détection basées sur les signatures. En employant un modèle Transformer basé sur CodeBERT, la recherche démontre que des règles YARA et Sigma anonymisées peuvent être attribuées à leurs auteurs originaux avec une grande précision, révélant ainsi un risque de sécurité opérationnelle (OPSEC) jusqu'alors négligé dans le partage de renseignements sur les menaces. Afin d'atténuer ces risques tout en préservant la sécurité collective, cette thèse introduit FLABELLA (Federated Learning Anomaly-Based Amender for Legitimate Labelling Algorithm). Ce cadre d'apprentissage fédéré (FL) fait passer l'approche défensive du partage de règles explicites à l'apprentissage collaboratif d'anomalies comportementales. Les résultats expérimentaux démontrent que FLABELLA traite efficacement les scénarios d'« attaque considérée comme bénigne » (AaB) ainsi que l'asymétrie des connaissances, réduisant de manière significative les faux négatifs et les faux positifs chez les clients décentralisés. Ces conclusions établissent une base solide pour une cybersécurité collaborative, sécurisée et respectueuse de la vie privée dans le paysage agricole en pleine mutation.

Summary:

The agricultural sector is experiencing rapid digital transformation into Agriculture 4.0, characterized by the integration of IoT devices, artificial intelligence, and autonomous machinery. This evolution has resulted in a complex, multi-provider ecosystem that is increasingly vulnerable to cyber threats. This thesis examines the effectiveness of Intrusion Detection Systems (IDS) within this resource-constrained and heterogeneous environment. The research initially identifies the operational challenges associated with deploying IDS in smart farming, including unique risks such as vulnerabilities in remote data logging and the security management of legacy ("brownfield") devices. To address the limitations of collaborative defense, the study quantifies the privacy risks linked to sharing signature-based detection rules. Employing a CodeBERT-based Transformer model, the research demonstrates that anonymized YARA and Sigma rules can be attributed to their original authors with high accuracy, thereby exposing a previously overlooked Operations Security (OPSEC) risk in threat intelligence sharing. To mitigate these risks while preserving collective security, this thesis introduces FLABELLA (Federated Learning Anomaly-Based Amender for Legitimate Labelling Algorithm). This Federated Learning (FL) framework transitions the defensive approach from sharing explicit rules to collaboratively learning behavioral anomalies. Experimental results demonstrate that FLABELLA effectively addresses "Attack as Benign" (AaB) scenarios and knowledge asymmetry, significantly reducing both false negatives and false positives across decentralized clients. These findings establish a robust foundation for secure, privacy-preserving, and collaborative cybersecurity in the evolving agricultural landscape.