جامعة محمد الخامس بالرباط
Université Mohammed V de Rabat

École Nationale Supérieure d'Informatique et d'Analyse des Systèmes

Centre d'Études Doctorales en Sciences des Technologies de l'Information et de l'Ingénieur

AVIS DE SOUTENANCE DE THÈSE DE DOCTORAT

Monsieur Mohammed CHEMMAKHA

Soutiendra publiquement sa thèse de Doctorat en Informatique

Le 31 décembre 2025 à 10h00 au Grand Amphi à l'ENSIAS de Rabat

Intitulé de la thèse

Advanced Intrusion Detection and Improving Generative Models for IoT Threat Mitigation

Président :

Pr. Moulay Ahmed FAQIHI, PES, ENSIAS, Université Mohammed V, Rabat

Directeur de thèse :

Pr. Mohamed LAZAAR, PES, ENSIAS, Université Mohammed V, Rabat

Rapporteurs :

Pr. Adil EL MAKRANI, MCH, Faculté des Sciences, Université Ibn Tofail, Kénitra

Pr. Zakariae EN-NAIMANI, MCH, ENSET Mohammedia, Université Hassan II

Pr. Raddouane CHIHEB, PES, ENSIAS, Université Mohammed V, Rabat

Examinateurs :

Pr. Youssef FAKHRI, PES, Faculté des Sciences, Université Ibn Tofail, Kénitra

Pr. Abderrahim EL QADI, PES, ENSAM, Université Mohammed V, Rabat

Invité :

Pr. Yassine AFOUDI, MC, Faculté des Sciences, Université Cadi Ayyad, Marrakech

Résumé :
La sécurisation des environnements de l'Internet des Objets (IoT) demeure un défi majeur en raison de l'hétérogénéité des dispositifs, du déséquilibre des données réseau et des ressources limitées. Dans ce travail, nous développons un cadre complet pour améliorer la détection d'intrusions dans les systèmes IoT. Nous construisons d'abord un ensemble de données optimisé en appliquant une sélection de caractéristiques de type embedded, afin de réduire la redondance et la complexité tout en préservant les informations essentielles. Nous générons ensuite des données synthétiques réalistes grâce à des modèles génératifs avancés tels que TGAN, CTGAN enrichi par des couches Conv1D, et TabSyn basé sur la diffusion, permettant d'équilibrer les classes et d'améliorer la qualité de l'apprentissage. Parallèlement, nous concevons des modèles de détection adaptés aux contraintes IoT. Nous exploitons des architectures GRU pour accélérer la génération de données, un modèle Attention Bi-LSTM pour renforcer la détection et réduire les faux positifs, ainsi qu'un classifieur LightGBM offrant rapidité et faible consommation mémoire. Les expérimentations menées sur UNSW-NB15 et NSL-KDD valident l'efficacité du cadre proposé, avec des améliorations significatives en précision, en stabilité et en détection des classes minoritaires. Ce travail ouvre la voie à des applications réelles et à des perspectives portant sur des modèles plus avancés et des déploiements pratiques dans des environnements IoT.
Mots-clés :
Détection d'intrusions, IoT, Données synthétiques, TGAN, CTGAN, TabSyn, Sélection de caractéristiques, GRU, Attention Bi-LSTM, LightGBM.

Abstract:
Securing Internet of Things (IoT) environments remains challenging due to heterogeneous devices, data imbalance, and limited computational capabilities. In this work, we develop a comprehensive framework to enhance intrusion detection in IoT systems. We first construct an optimized dataset by applying embedded feature-selection methods to reduce redundancy and complexity while preserving essential information. We then generate realistic synthetic data using advanced generative models such as TGAN, CTGAN enhanced with Conv1D layers, and the diffusion-based TabSyn, enabling better class balancing and improved training quality. In parallel, we design detection models adapted to IoT constraints. GRU architectures are employed to speed up data generation, an Attention-based Bi-LSTM improves detection performance and reduces false positives, and a LightGBM classifier ensures fast learning with low memory consumption. Experiments conducted on UNSW-NB15 and NSL-KDD confirm the effectiveness of the proposed framework, showing significant gains in accuracy, stability, and minority-class detection. This work opens the way to real-world applications and future extensions involving more advanced models and practical IoT deployments.
Keywords:
Intrusion detection, IoT, Synthetic data, TGAN, CTGAN, TabSyn, Feature selection, GRU, Attention Bi-LSTM, LightGBM.