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

MADAME Habiba BOUIJIJ

Soutiendra publiquement sa thèse de Doctorat en Informatique

Le Mercredi 31 Juillet 2024 à 11h00 au Grand Amphi de l'ENSIAS de Rabat

Intitulé de la thèse

Enhancing Cybersecurity through the Integration of Artificial Intelligence: Advanced Detection of Phishing URL and DDOS Attacks

Président :

Pr. Ilham BERRADA, PES, ENSIAS, Université Mohammed V de Rabat

Directeur de thèse :

Pr. Amine BERQIA, PES, ENSIAS, Université Mohammed V de Rabat

Rapporteurs :

Pr. Mohamed Dafir ECH-CHRIF EL KETTANI, PES, ENSIAS, Université Mohammed V de Rabat

Pr. Mohamed ET-TOLBA, PES, Institut National des Postes et Télécommunications, Rabat

Pr. Ali KARTIT, PES, ENSA, Université Chouaib Doukkali, El Jadida

Examinateur :

Pr. Hanan EL BAKKALI, PES, ENSIAS, Université Mohammed V de Rabat

Résumé : À l'ère numérique actuelle, la cybersécurité est devenue essentielle pour protéger les infrastructures critiques, les données personnelles et les secrets d'entreprise. La rapidité des avancées technologiques a conduit à des cyberattaques de plus en plus complexes et nombreuses, mettant à l'épreuve les méthodes traditionnelles de sécurité informatique. Parmi les menaces les plus répandues et les plus dévastatrices figurent les URL de phishing et les attaques DDoS. Cette thèse se consacre au développement minutieux et à l'analyse de modèles d'apprentissage automatique (ML) et d'apprentissage profond (DL) conçus pour détecter rapidement et avec précision ces types d'attaques. Avec l'augmentation constante des cyberattaques, la nécessité de concevoir des systèmes de sécurité efficaces et réactifs est plus urgente que jamais.

Notre recherche se concentre sur l'étude et la mise en oeuvre de diverses architectures et algorithmes, utilisant des techniques de ML telles que les forêts aléatoires (RF), les arbres de décision (DT), les arbres extrêmement aléatoires (ET), les k-plus proches voisins (KNN), Adaboost, et la régression logistique (LR). Nous intégrons également des modèles de deep learning tels que les réseaux de neurones denses (DNN), les réseaux de neurones convolutifs (CNN), et les réseaux de neurones à mémoire à court et long terme (LSTM).

À travers des études de cas pratiques, notre recherche démontre comment ces techniques peuvent renforcer la sécurité des systèmes de l'Internet des Objets (IoT), souvent vulnérables aux cyberattaques en raison de leur nature interconnectée et de normes de sécurité parfois inadéquates. Cette étude fournit une évaluation quantitative des performances de ces modèles, mesurant leur précision, leur rapidité et leur fiabilité, et discute également de leur intégration pratique dans des systèmes de sécurité opérationnels pour l'IoT.

Mots-clés: Apprentissage automatique, Apprentissage profond, Attaques, Classification, Cybersécurité, DoS/DDoS, Hameçonnage, , Internet des objets, Intrusion, Détection

Abstract: In today's digital era, cybersecurity has become essential for protecting critical infrastructure, personal data, and corporate secrets. Technological advancement has led to increasingly complex and numerous cyberattacks, challenging traditional IT security methods. Among the most widespread and devastating threats are phishing URLs and DDoS attacks. This thesis is dedicated to the meticulous development and analysis of machine learning (ML) and deep learning (DL) models designed to swiftly and accurately detect these attacks. With the constant rise in cyberattacks, designing effective and responsive security systems is more urgent than ever.

Our research focuses on studying and implementing various architectures and algorithms, employing ML techniques such as Random Forests (RF), Decision Trees (DT), Extremely Randomized Trees (ET), k-Nearest Neighbors (KNN), Adaboost (AB), and Logistic Regression (LR). Additionally, we integrate deep learning models like Dense Neural Networks (DNN), Convolutional Neural Networks (CNN), and Long Short-Term Memory Networks

(LSTM). Through practical case studies, our research demonstrates how these techniques can enhance the security of Internet of Things (IoT) systems, which are often vulnerable to cyberattacks due to their interconnected nature and sometimes inadequate security standards. This study provides a quantitative evaluation of the performance of these models, measuring their accuracy, speed, and reliability, and also discusses their practical integration into operational security systems for IoT.

Keywords: Attacks; Classification; Cybersecurity; Detection; Deep Learning; DoS/DDoS; Machine Learning; Phishing; Internet of Thing; Intrusion