Nom et Prénom : BENADDI HAFSA
Date de soutenance : 22/12/2022
Directeur de Thèse : IBRAHIMI KHALIL

Sujet de Thèse :

Advaces in Cybersecurity Management based Instrusion Detection Systems for Internet of Things using Machine Learning, Stochastic Game and Blockchain

Résumé :

Au fur et à mesure de la croissance des développements technologiques, il existe plusieurs problèmes et défis de sécurité auxquels sont confrontés les cadres de l'Internet des objets (IoT) où le but est l'échelle massive des objets et l'hétérogénéité. Certaines études en cours pour améliorer la sécurité de l'IoT incluent diverses approches pour assurer la sécurité des données telles que la confidentialité, l'authentification, l'intégrité et le contrôle d'accès à l'intérieur des réseaux IoT, la confidentialité et la confiance entre les utilisateurs et les objets, et l'application des politiques de sécurité et de confidentialité. Cependant, même avec les composants mentionnés ci-dessus, l'infrastructure critique IdO est vulnérable à de multiples attaques et les utilisateurs criminels visant à endommager le réseau, les systèmes de détection d'intrusion (IDS) sont largement utilisés et mis en œuvre dans divers réseaux (c'est-à-dire financiers, de sécurité et organismes de sécurité) pour surveiller le réseau d'activités anormales et normales. Dans cette thèse, nous étudions le problème du provisionnement de la sécurité dans l'IoT. Nous proposons divers schémas IDS combinés basés sur l'apprentissage automatique (ML) pour exploiter la puissance de l'IoT, offrant des qualités pour examiner efficacement tout le trafic à travers l'IoT. Nous présentons également de nouveaux cadres pour détecter les anomalies dans les réseaux IoT en utilisant le réseau antagoniste génératif (GAN) pour créer des distributions réalistes pour un ensemble de fonctionnalités donné afin de surmonter le problème du déséquilibre des données. Cependant, nous présentons une analyse approfondie de l'utilisation de l'apprentissage automatique, de l'apprentissage en profondeur, de l'apprentissage automatique contradictoire, de l'apprentissage par renforcement et des solutions Blockchain pour reconnaître les comportements intrusifs dans le réseau surveillé.

Abstract:

The proliferation of cyber-treats in several Internet of things (IoT) has raised significant concerns among the field experts as it poses a major challenge in the IoT networks. Besides, using a sophisticated and modern network in major companies, critical information becomes vulnerable to intrusions and attacks. However, to detect these threats of attacks, Intrusion Detection Systems (IDS) are extensively used and implemented in diverse networks (i.e., financial, security, and safety organizations) to monitor the abnormal and normal activities network. In this thesis, we investigate the problem of security provisioning in IoT. We propose various combined Machine Learning (ML)-driven IDSs schemes for harnesses the power of the IoT, providing qualities to efficiently examine all traffic across the IoT. We also present a novel frameworks for detecting anomalies in IoT networks utilizing Generative Adversarial Network (GAN) to build realistic distributions for a given feature set to overcome the issue of data imbalance. However, we present an in-depth analysis of the use of machine learning, deep learning, adversarial machine learning, reinforcement learning, and Blockchain solutions to recognize intrusive behaviours in the monitored network.