الجمهورية الشعبية الديمقراطية الجزائرية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة العليا للإعلام الآلي ٠08 ماي 5491٠ بسيدي بلعباس
École Supérieure en Informatique
-08 Mai 1945- Sidi Bel Abbès

MEMOIRE

Pour En Vue de l'obtention du diplôme de **Master**
Filière:: **Informatique**
Spécialité: **Système d'Information et Web (SIW)**

Thème

Anomaly Detection using AutoEncoders: The advanced Persistent Threats case

---

Présenté par:
BOUDOUARA Nadjet
LAIB Oumaima

Soutenu le 04 Juillet 2022 Devant le jury composé de:

Dr. KECHAR Mohamed	President
Dr. BENABDERRAHMANE Sid Ahmed	Encadreur
Pr. BENSLIMANE Sidi Mohamed	Co-Encadreur
Dr. KHALDI Miloud	Examinateur

Année Universitaire : 2021/2022

Abstract

In the recent decade, there has been a massive increase in the number of apps with linked users and services for that Anomaly detection became a significant subject that has been studied in a variety of academic fields and application domains. Many anomaly detection approaches have been developed expressly for certain application areas, while others are more general.This study aims to give an organized and thorough review of anomaly detection research. We classified existing approaches into several groups depending on the underlying strategy used by each technique.

We defined essential assumptions for each category that are employed by the strategies to distinguish between normal and abnormal behavior. We propose a fundamental anomaly detection approach for each category and then illustrate how the many current techniques in that category are modifications of the basic technique. This template simplifies and condenses comprehension of the procedures in each area.

We believe that this study will give a better knowledge of the various areas in which research on this issue has been conducted, as well as how approaches created in one field can be utilized in domains for which they were not originally intended.

Keywords: Anomaly detection, Machine learning, Deep learning, cybersecurity, Advanced persistent threats, Big Data, Autoencoder.

Résumé

Au cours de la dernière décennie, il y a eu une augmentation massive du nombre d'applications avec des utilisateurs et des services liés pour que la détection d'anomalies soit devenue un sujet important qui a été étudié dans une variété de domaines académiques et de domaines d'application. De nombreuses approches de détection d'anomalies ont été développées expressément pour certains domaines d'application, tandis que d'autres sont plus générales. Cette étude vise à donner un examen organisé et approfondi de la recherche sur la détection d'anomalies. Nous avons classé les approches existantes en plusieurs groupes en fonction de la stratégie sous-jacente utilisée par chaque technique.

Nous avons défini des hypothèses essentielles pour chaque catégorie qui sont employées par les stratégies pour faire la distinction entre un comportement normal et anormal.

Nous proposons une approche fondamentale de détection des anomalies pour chaque catégorie, puis illustrons comment les nombreuses techniques actuelles de cette catégorie sont des modifications de la technique de base. Ce modèle simplifie et condense la compréhension des procédures dans chaque domaine. Nous croyons que cette étude permettra de mieux connaître les différents domaines dans lesquels la recherche sur cette question a été menée, ainsi que la façon dont les approches créées dans un domaine peuvent être utilisées dans des domaines pour lesquels elles n'étaient pas initialement destinées.

Mot Clé : Détection d'anomalies, Machine learning, Deep learning , cybersécurité, Menaces persistantes avancées, Big Data, Autoencodeur.