# Intrusion Detection Using Machine Learning and Feature Selection Based on Enhancing Chernobyl Disaster Optimizer Algorithm

**Prepared by**

**Ibrahim Mousa AL-Shibly**

**Supervisor by**

**Dr. Mahmoud Ahmad Omari**

## Abstract

Artificial Intelligence (AI) is a powerful technology that has the potential to completely transform cybersecurity, by enhancing malware detection and strengthening defenses against cyberattacks. In this study, explore the application of a binary version of the Chernobyl Disaster Optimizer (CDO) algorithm to tackle the feature selection problem in intrusion detection system (IDS) classification. The key innovation in this work lies in the conversion of the original continuous CDO algorithm into a binary optimization technique specifically tailored for the feature selection task. By converting the search space from continuous to binary, the binary CDO algorithm was able to better handle the inherent binary nature of the feature selection problem, leading to more efficient and effective feature subset identification. The experimental results demonstrate the superior performance of the binary CDO algorithm, coupled with a wrapper method (Random Forest) and sigmoid transfer function with balancing, compared to other feature selection techniques. This approach

outperformed the other methods across various performance metrics, including accuracy, precision, recall, and F1-score.

The binary CDO algorithm ability to select the most relevant features for the IDS prediction model played a crucial role in improving the overall performance of the classifiers. The Random Forest model, enhanced by the binary CDO-based feature selection, emerged as the top performer, achieving the highest accuracy of 93.83% and an exceptional F1-score of 94.48%. These findings underscore the significance of feature selection in enhancing the performance of IDS prediction models, and the binary CDO algorithm's ability to identify the most informative features, ultimately leading to improved cybersecurity solutions.

The insights gained from this research contribute substantially to the ongoing advancements in AI-driven cybersecurity. By harnessing the power of binary optimization techniques, such as the binary CDO algorithm, and integrating them with robust machine learning models.

**Keywords: Cybersecurity, Machine Learning, Feature Selection, Binary Optimization Algorithm, Classification, Chernobyl Disaster Optimizer, CDO.**

# كشف التسلل باستخدام التعلم الآلي واختيار الميزات بناءً على تحسين خوارزمية كارثة شارنوبل

**إعداد**

**ابراهيم موسى الشبلي**

**إشراف**

**الدكتور محمود العمري**

## الملخص

الذكاء الاصطناعي (AI) هو تقنية قوية لديها القدرة على إحداث تحول كامل في الأمن السيبراني، من خلال تعزيز اكتشاف البرامج الضارة وتعزيز الدفاعات ضد الهجمات السيبرانية. في هذه الدراسة، استكشاف تطبيق نسخة ثنائية من خوارزمية Chernobyl Disaster Optimizer (CDO)لمعالجة مشكلة اختيار الميزة في تصنيف نظام كشف التسلل (IDS). يكمن الابتكار الرئيسي في هذا العمل في تحويل خوارزمية CDO المستمرة الأصلية إلى تقنية تحسين ثنائية مصممة خصيصًا لمهمة اختيار الميزات. من خلال تحويل مساحة البحث من مستمر إلى ثنائي، تمكنت خوارزمية CDO الثنائية من التعامل بشكل أفضل مع الطبيعة الثنائية المتأصلة لمشكلة اختيار الميزة، مما يؤدي إلى تحديد مجموعة فرعية أكثر كفاءة وفعالية. توضح النتائج التجريبية الأداء المتفوق لخوارزمية CDO الثنائية، إلى جانب طريقة التغليف (الغابات العشوائية) ووظيفة النقل السيني مع الموازنة، مقارنة بتقنيات اختيار الميزات الأخرى. وقد تفوق هذا النهج على الطرق الأخرى عبر مقاييس الأداء المختلفة، بما في ذلك الدقة والدقة والاستدعاء ودرجة.F1

لعبت قدرة خوارزمية CDO الثنائية على تحديد الميزات الأكثر صلة بنموذج التنبؤ IDS دورًا حاسمًا في تحسين الأداء العام للمصنفات. برز نموذج Random Forest ، المعزز باختيار الميزات الثنائية المستندة إلىCDO ، كأفضل أداء محققًا أعلى دقة بنسبة 93.83% ودرجة F1 استثنائية تبلغ 94.48%. تؤكد هذه النتائج على أهمية اختيار الميزات في تعزيز أداء نماذج التنبؤ IDS، وقدرة خوارزمية CDO الثنائية على تحديد الميزات الأكثر إفادة، مما يؤدي في النهاية إلى تحسين حلول الأمن السيبراني.

تساهم الأفكار المكتسبة من هذا البحث بشكل كبير في التقدم المستمر في مجال الأمن السيبراني المعتمد على الذكاء الاصطناعي. من خلال تسخير قوة تقنيات التحسين الثنائية، مثل خوارزمية CDO الثنائية، ودمجها مع نماذج قوية للتعلم الآلي.

**الكلمات المفتاحية: الأمن السيبراني، التعلم الآلي، اختيار الميزات، خوارزمية التحسين الثنائي، التصنيف، محسن كارثة تشيرنوبيل، CDO**.