Leveraging Network Vulnerability Detection using Improved Import Vector Machine and Cuckoo Search based Grey Wolf Optimizer

Publisher: IEEE Cite This PDF

P. Preethi ; I Vasudevan ; S Saravanan ; R Krishna Prakash ; A Devendhiran All Authors

9 Cites in Papers
37 Full Text Views

Abstract
Document Sections
I. Introduction
II. Related Works
III. Proposed methodology for IDS
IV. Experimental results
V. Conclusion
Authors
Figures
References
Citations
Keywords
Metrics
More Like This

Abstract:
In the current interconnected and susceptible digital environment, the demand for reliable network attack prediction systems has reached a critical level. This research paper presents a novel approach for network intrusion detection utilizing the Improved Import Vector Machine (IVM) classification algorithm combined with feature selection using Cuckoo Search based Grey Wolf Optimization (CS-GWO). The aim is to improve the accuracy and effectiveness of intrusion detection systems by selecting the most relevant features and employing a powerful classification algorithm. The proposed methodology begins with data preprocessing, ensuring the dataset is appropriately cleaned and normalized. Subsequently, the CS-GWO algorithm is applied for feature selection, leveraging the strengths of both Cuckoo Search and Grey Wolf Optimization. This hybrid approach efficiently explores the search space to identify the optimal feature subset that contributes to accurate intrusion detection. Once the feature selection process is completed, the IVM classification algorithm is employed to classify network instances into intrusion or normal categories. The IVM algorithm is chosen for its ability to handle high-dimensional data and its robustness in dealing with imbalanced datasets commonly encountered in network intrusion detection. To evaluate the performance of the proposed approach, extensive experiments are conducted using benchmark datasets. Various evaluation metrics such as accuracy, precision, recall, and F1 score are utilized to assess the effectiveness of the system in detecting network intrusions. The results demonstrate that the combination of IVM classification and CS-GWO feature selection significantly improves the accuracy and efficiency of network intrusion detection. The selected features obtained through CS-GWO contribute to enhanced classification performance, enabling the system to accurately identify and respond to potential intrusions in real-time scenarios.

Show More

Published in: 2023 1st International Conference on Optimization Techniques for Learning (ICOTL)

Date of Conference: 07-08 December 2023

DOI: 10.1109/ICOTL59758.2023.10435119

Date Added to IEEE *Xplore*: 19 February 2024

Publisher: IEEE

ISBN Information:

Conference Location: Bengaluru, India

Recommended for You (Beta)

Improving IoT Security - A Smart Intrusion Detection System Utilizing Deep…

A CNN-IOT Model for Suspicious Behaviour Detection of People by Surveillance using ML and DL

Intelligent IoT: Leveraging Data Analysis, Computer Vision, and Machine Learning for Smart…

Learn More

Sign in to Continue Reading

Authors

Figures

References

Citations

Keywords

Metrics



IEEE Personal Account

CHANGE USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS

VIEW PURCHASED DOCUMENTS

Profile Information

COMMUNICATIONS PREFERENCES

PROFESSION AND EDUCATION

TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800 678 4333

WORLDWIDE: +1 732 981 0060

CONTACT & SUPPORT

Follow

About IEEE *Xplore* | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | IEEE Ethics Reporting | Sitemap | IEEE Privacy Policy

A public charity, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2026 IEEE - All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies.