



All



ADVANCED SEARCH

Conferences > 2023 12th International Confe... ?

# Geometric Structure Based Feature Transformation for Network Anomaly Detection System

Publisher: IEEE

Cite This



A.S Aneetha All Authors ...



33 Full Text Views

## Alerts

Manage Content Alerts Add to Citation Alerts

### Abstract

#### Document Sections

- I Introduction
- II Methods and Materials
- III Proposed HAMD Model
- IV Experiments and Results
- V Conclusion

Authors

Figures

References

Keywords

Metrics



Download PDF

#### Abstract:

Due to development of new internet connected devices, the attack surface has also been increased for the cyber intruders. The evolution of these cyber intruders poses a ... **View more**

#### Metadata

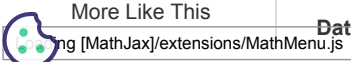
##### Abstract:

Due to development of new internet connected devices, the attack surface has also been increased for the cyber intruders. The evolution of these cyber intruders poses a critical challenge for designing of detection mechanisms especially in network devices. Intrusion detection system is one such approach with the ability of detecting dynamic and unknown attacks. In this work, network anomaly detection system is developed using Mahalanobis distance-based detection mechanism with heron's triangle area based transformed features. The KDD Cup'99 network dataset is utilized to analysis the performance of the system. It contains four different attack types such as DoS, Probe, R2L and U2R. The model has achieved very high detection rate for Normal and U2R classes with false alarm rates of 1.53% and 6.66% respectively. The detection rates are more than 99.53%, 99.7% and 98% for Probe, DoS and R2L classes along with 0.09%, 0.66% and 0.2% false alarm rates respectively.

Published in: 2023 12th International Conference on Advanced Computing (ICoAC)

Date of Conference: 17-19 August 2023

DOI: 10.1109/ICoAC59537.2023.10249601



Date Added to IEEE Xplore: 19 September 2023

Publisher: IEEE

► ISBN Information:

Conference Location: Chennai, India

### ☰ Contents

#### I Introduction

In recent years due to pandemic situation, there is an exponential growth of computer devices and a network technology, made the network security has become most significant in cyber systems. Many network intrusion detection systems are available to detect the attacks of known signatures, whereas there is a great challenge in detecting new born or zero-day attacks. Development of efficient Intrusion Detection Systems (IDS) to provide real time dynamic security for all internet connect devices and network technologies assumes greater importance [1]. An intrusion detection system consists of relevant security features capable of adapting themselves for the changing environment based on their learning ability of events from time to time. IDS is categorized into signature and anomaly detection, where signature has the ability of detecting known intrusion patterns whereas anomaly is capable of detection zero-day attacks [2].

Sign in to Continue Reading

Authors



Figures



References



Keywords



Metrics



#### More Like This

Network Intrusion Detection System for Feature Extraction Based on Machine Learning Techniques

2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA)

Published: 2023

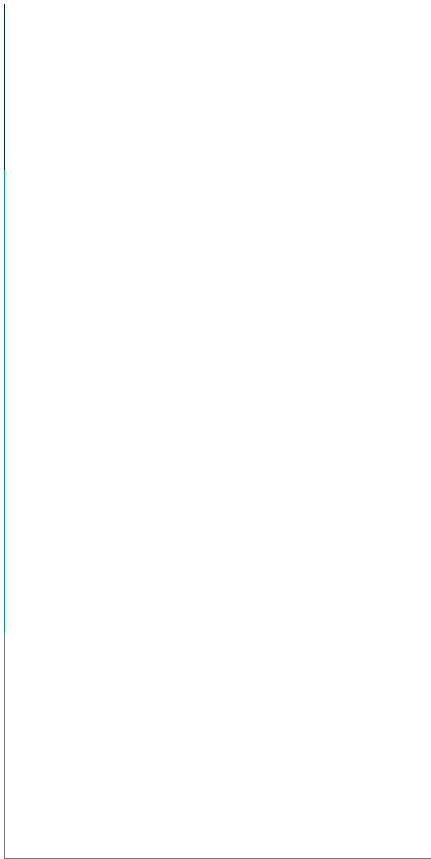
Ensemble of binary SVM classifiers based on PCA and LDA feature extraction for intrusion detection

2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)

Published: 2016

Show More

Loading [MathJax]/extensions/MathMenu.js



**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 not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2024 IEEE - All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies.

**IEEE Account**

- » [Change Username/Password](#)
- » [Update Address](#)

**Purchase Details**

- » [Payment Options](#)
- » [Order History](#)
- » [View Purchased Documents](#)

**Profile Information**

- » [Communications Preferences](#)
- » [Profession and Education](#)

Loading [MathJax]extensions/MathMenu.js

» Technical Interests

**Need Help?**

» **US & Canada:** +1 800 678 4333

» **Worldwide:** +1 732 981 0060

» Contact & Support

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2024 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.