

1 document have cited:

Deep Learning-Based Intrusion Detection Model for Network Security
 Pande S.D., Lanke G.R., Soni M., Kulkarni M.A., Maaliw R.R., Singh P.P.
 (2023) Lecture Notes in Networks and Systems, 699 LNNS , pp. 377-386.

Search within results...



Refine results

Limit to Exclude

Open Access

- ☐ All Open Access (1) >
- ☐ Hybrid Gold (1) >

Learn more

Year

- ☐ 2024 (1) >

Author name

- ☐ Khalaf, A.O.A.H. (1) >
- ☐ Mohamed, R. (1) >
- ☐ Raziff, A.R.A. (1) >

Subject area

- ☐ Multidisciplinary (1) >

Document type

- ☐ Article (1) >

Source title

- ☐ Journal Of Advanced Research In Applied Sciences And Engineering Technology (1) >

Publication stage

- ☐ Final (1) >

Keyword

- ☐ Imbalance Dataset (1) >
- ☐ Intrusion Detection (1) >
- ☐ LSTM (1) >
- ☐ SMOTE (1) >

Affiliation

- ☐ International Islamic University Malaysia (1) >
- ☐ Universiti Putra Malaysia (1) >

Funding sponsor

- ☐ (1) >

Analyze search results

Hide all abstracts Sort on: Date (newest)



☐ All Export Download View citation overview View cited by Save to list ...

	Document title	Authors	Year	Source	Cited by
<input type="checkbox"/> 1	Detection Model for Ambiguous Intrusion using SMOTE and LSTM for Network Security <i>Open Access</i>	Khalaf, A.-O.A.H., Mohamed, R., Raziff, A.R.A.	2024	Journal of Advanced Research in Applied Sciences and Engineering Technology 39(2), pp. 191-203	0

Hide abstract ^ [View at Publisher](#) [Related documents](#)

In today's interconnected world, networks play a crucial role. Consequently, network security has become increasingly vital. To ensure network security, various methods are employed, including digital signatures, firewalls, and intrusion detection. Among these methods, intrusion detection systems have gained significant popularity due to their ability to identify new attacks. However, the accuracy of these systems still requires further improvement. One of the challenges is the potential bias introduced by using imbalance datasets that contains more information on normal activities than on attacks. To address it, SMOTE method was proposed and additionally, the study explores the use of Long Short-Term Memory (LSTM) for classification purposes. The experiments are conducted using two datasets: UNSW NB-15 and CICIDS 2017. The results obtained demonstrate that the proposed methods achieve an accuracy of 96% with the UNSW NB-15 dataset and 99% with the CICIDS 2017 dataset. These findings indicate an improvement of 3% and 1% respectively compared to existing literature.

Display: 20 results per page

1

^ Top of page

Undefined

(1) >

Country/territory

^

Malaysia

(1) >

Source type

^

Journal

(1) >

Language

^

English

(1) >

Limit to

Exclude

[Restore original settings](#)

[↗ Export refine](#)

About Scopus

- [What is Scopus](#)
- [Content coverage](#)
- [Scopus blog](#)
- [Scopus API](#)
- [Privacy matters](#)

Language

- [日本語版を表示する](#)
- [查看简体中文版本](#)
- [查看繁體中文版本](#)
- [Просмотр версии на русском языке](#)

Customer Service


- [Help](#)
- [Tutorials](#)
- [Contact us](#)

ELSEVIER

[Terms and conditions](#)

[Privacy policy](#)

All content on this site: Copyright © 2024 Elsevier B.V., its licensors, and contributors. All rights are reserved, including those for text and data mining, AI training, and similar technologies. For all open access content, the Creative Commons licensing terms apply. We use cookies to help provide and enhance our service and tailor content.By continuing, you agree to the [use of cookies](#).

RELX™