Lecture Notes in Networks and Systems . Volume 699 LNNS, Pages 377 - 386 . 2023 . Intelligent Computing and Networking - Proceedings of IC-ICN 2023 . Mumbai . 24 February 2023through 25 February 2023 . Code 299239

Deep Learning-Based Intrusion Detection Model for Network Security

Pande, Sagar Dhanraj[a] ; Lanke, Govinda Rajulu[b]; Soni, Mukesh[c]; Kulkarni, Mukund Anant[d]; Maaliw, Renato R.[e] ; Singh, Pavitar Parkash[f]

Save all to author list

[a] School of Computer Science and Engineering, VIT-AP University, Andhra Pradesh, Amaravati, India
[b] Data Science and Engineering, Birla Institute of Technology and Science, Rajasthan, Pilani, India
[c] University Centre for Research and Development Chandigarh University, Punjab, Mohali, 140413, India
[d] Bharati Vidyapeeth (Deemed to Be University), Institute of Management, Kolhapur, India

View additional affiliations

Document type
Conference Paper

Source type
Book Series

ISSN
23673370

ISBN
978-981993176-7

DOI
10.1007/978-981-99-3177-4_27

View more

1 85th percentile Citation in Scopus | 1.96 FWCI | View all metrics

Full text options Export

Abstract

Since it serves as a potent means of network security defence, intrusion detection technology is an essential component of the network security system. As the Internet has grown quickly, so too have network data volumes and threats, which are now more sophisticated and diversified. Modern intrusion detection equipment cannot reliably recognize different types of attacks. A CBL_DDQN intrusion detection model based on an upgraded double deep Q network is suggested based on deep reinforcement learning to address the imbalance of regular traffic and attack traffic data in the actual network environment as well as the low detection rate of attack traffic. This model integrates the feedback learning and policy-generating methods of deep reinforcement learning with a one-dimensional convolutional neural network and a bidirectional long-term, short-term memory network to train agents to attack different types of samples. Classification, to some extent, lessens the reliance on data labels during model training. The Borderline-SMOTE algorithm reduces data imbalance, thereby improving the detection rate of rare attacks. The NSL KDD and UNSW NB15 data sets are used to assess the model's efficacy. The findings demonstrate that the model has performed well with respect to the three indices of accuracy, precision, and recall, and the detection effect is significantly superior to Adam BNDNN, KNN, SVM, etc. The detection method is an efficient network intrusion detection model. © 2023, The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd.

Author keywords

Classification; CNN; Deep learning; Intrusion detection; LSTM; SMOTE

Indexed keywords

SciVal Topics

Metrics

References (30)

View in search results format

All Export Print E-mail Save to PDF Create bibliography

1 Haghighat, M.H., Li, J.
Intrusion detection system using voting-based neural network (Open Access)

(2021) *Tsinghua Science and Technology*, 26 (4), art. no. 9312777, pp. 484-495. Cited 45 times.
http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=5971803
doi: 10.26599/TST.2020.9010022

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

- Undefined (1)

Analyze search results

Hide all abstracts Sort on: Date (newest)

All Export Download Citation overview View cited by Save to list

	Document title	Authors	Year	Source	Cited by
1	Detection Model for Ambiguous Intrusion using SMOTE and LSTM for Network Security *Open Access*	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

Journal of Advanced Research in Applied Sciences and Engineering Technology • *Open Access* • Volume 39, Issue 2, Pages 191 - 203 • September 2024

Document type
Article • *Hybrid Gold Open Access*

Source type
Journal

ISSN
24621943

DOI
10.37934/araset.39.2.191203

View more

Detection Model for Ambiguous Intrusion using SMOTE and LSTM for Network Security

Khalaf, Al-Ogaidi Ali Hameed[a];

Mohamed, Raihani[a] ; Raziff, Abdul Rafiez Abdul[b]

Save all to author list

[a] Department of Computer Science, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, UPM, Selangor, Serdang, 43400, Malaysia

[b] Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Kuala Lumpur, 50728, Malaysia

Full text options Export

Abstract

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.

Author keywords

imbalance dataset; Intrusion detection; LSTM; SMOTE

SciVal Topics

Metrics

References (20)

View in search results format >

All Export Print E-mail Save to PDF Create bibliography

1 Lazarevic, Aleksandar, Kumar, Vipin, Srivastava, Jaideep
Intrusion detection: A survey
(2005) *Managing Cyber Threats: Issues, Approaches, and Challenges*, pp. 19-78. Cited 163 times.
https://doi.org/10.1007/0-387-24230-9_2

2 Taghavinejad, S.M., Taghavinejad, M., Shahmiri, L., Zavvar, M., Zavvar, M.H.
Intrusion Detection in IoT-Based Smart Grid Using Hybrid Decision Tree
(2020) *2020 6th International Conference on Web Research, ICWR 2020*, art. no. 9122320, pp. 152-156. Cited 37 times.
http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=9118608
ISBN: 978-172811051-6
doi: 10.1109/ICWR49608.2020.9122320
View at Publisher

3 Liang, X., Li, D., Sengi, M., Madden, A., Ding, Y., Bu, Y.

Liang, X., Li, D., Songi, M., Madden, A., Ding, Y., Bu, Y.

Predicting biomedical relationships using the knowledge and graph embedding cascade model

(2019) *PLoS ONE*, 14 (6), art. no. e0218264. Cited 23 times.
https://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0218264&type=printable
doi: 10.1371/journal.pone.0218264

View at Publisher

4 Ariffin, N.A.M., Paliah, V.

An Improved Secure Authentication in Lightweight IoT

(2023) *Journal of Advanced Research in Applied Sciences and Engineering Technology*, 31 (3), pp. 191-207.
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/article/view/1959
doi: 10.37934/araset.31.3.191207

View at Publisher

5 Mohamed, R., Perumal, T., Sulaiman, M.N., Mustapha, N., Razali, M.N.

Conflict resolution using enhanced label combination method for complex activity recognition in smart home environment (Open Access)

(2017) *2017 IEEE 6th Global Conference on Consumer Electronics, GCCE 2017*, 2017-January, pp. 1-3. Cited 8 times.
ISBN: 978-150904045-2
doi: 10.1109/GCCE.2017.8229477

View at Publisher

6 Zainudin, M.N.S., Sulaiman, M.N., Mustapha, N., Perumal, T., Mohamed, R.

Recognizing complex human activities using hybrid feature selections based on an accelerometer sensor (Open Access)

(2017) *International Journal of Technology*, 8 (5), pp. 968-978. Cited 6 times.
https://ijtech.eng.ui.ac.id/
doi: 10.14716/ijtech.v8i5.879

View at Publisher

7 Nassar, M., El-Bahnasawy, N.A., Ahmed, H.-D.H., Saleeb, A.A., El-Samie, F.E.A.

Network intrusion detection, literature review and some techniques comparision

(2019) *ICENCO 2019 - 2019 15th International Computer Engineering Conference: Utilizing Machine Intelligence for a Better World*, art. no. 9027296, pp. 62-71. Cited 5 times.
http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=9017210
ISBN: 978-172815146-5
doi: 10.1109/ICENCO48310.2019.9027296

View at Publisher

8 Salih, A.A., Abdulazeez, A.M.

Evaluation of Classification Algorithms for Intrusion Detection System: A Review

(2021) *Journal of Soft Computing and Data Mining*, 2 (1), pp. 31-40. Cited 52 times.
https://publisher.uthm.edu.my/ojs/index.php/jscdm/article/download/7982/4200
doi: 10.30880/jscdm.2021.02.01.004

View at Publisher

9 Bhosale, K.S., Nenova, M., Iliev, G.

Data Mining Based Advanced Algorithm for Intrusion Detections in Communication Networks (Open Access)

(2018) *Proceedings of the International Conference on Computational Techniques, Electronics and Mechanical Systems, CTEMS 2018*, art. no. 8769173, pp. 297-300. Cited 14 times.
http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=8765670
ISBN: 978-153867709-4
doi: 10.1109/CTEMS.2018.8769173

View at Publisher

10 Gulla, K.K., Viswanath, P., Veluru, S.B., Kumar, R.R.

Machine learning based intrusion detection techniques (Open Access)

(2019) *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, pp. 873-888. Cited

11 times.
http://dx.doi.org/10.1007/978-3-030-22277-2
ISBN: 978-303022277-2; 978-303022276-5
doi: 10.1007/978-3-030-22277-2_35

View at Publisher

11 Pande, S.D., Lanke, G.R., Soni, M., Kulkarni, M.A., Maaliw, R.R., Singh, P.P.

Deep Learning-Based Intrusion Detection Model for Network Security (Open Access)

(2023) *Lecture Notes in Networks and Systems*, 699 LNNS, pp. 377-386.
https://www.springer.com/series/15179
ISBN: 978-981993176-7
doi: 10.1007/978-981-99-3177-4_27

View at Publisher

12 Gu, J., Lu, S.

An effective intrusion detection approach using SVM with naïve Bayes feature embedding

(2021) *Computers and Security*, 103, art. no. 102158. Cited 188 times.
https://www.journals.elsevier.com/computers-and-security
doi: 10.1016/j.cose.2020.102158

View at Publisher

13 Ramasubramanian, G., Rajaprakash, S.

An Avant-Garde African Vulture Optimization (A^2 VO) based Deep RNN-LSTM Model for 5G-IoT Security

(2023) *Journal of Advanced Research in Applied Sciences and Engineering Technology*, 32 (1), pp. 1-17. Cited 2 times.
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/article/view/2941/2312
doi: 10.37934/ARASET.32.1.117

View at Publisher

14 Taher, K.A., Mohammed Yasin Jisan, B., Rahman, M.M.

Network intrusion detection using supervised machine learning technique with feature selection (Open Access)

(2019) *1st International Conference on Robotics, Electrical and Signal Processing Techniques, ICREST 2019*, art. no. 8644161, pp. 643-646. Cited 153 times.
http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=8640012
ISBN: 978-153868012-4
doi: 10.1109/ICREST.2019.8644161

View at Publisher

15 Chkirbene, Z., Eltanbouly, S., Bashendy, M., Alnaimi, N., Erbad, A.

Hybrid Machine Learning for Network Anomaly Intrusion Detection

(2020) *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies, ICIoT 2020*, art. no. 9089575, pp. 163-170. Cited 43 times.
http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=9081868
ISBN: 978-172814821-2
doi: 10.1109/ICIoT48696.2020.9089575

View at Publisher

16 Wang, H., Xu, Q., Zhou, L.

Seminal quality prediction using clustering-based decision forests (Open Access)

(2014) *Algorithms*, 7 (3), pp. 405-417. Cited 15 times.
http://www.mdpi.com/1999-4893/7/3/405/pdf
doi: 10.3390/a7030405

View at Publisher

17 Mohamed, R., Raziff, A.R.A., Nasir, S.M.

A RESAMPLE-SMOTE BALANCE WITH RANDOM FOREST FOR IMPROVING SEMINAL QUALITY PREDICTION IN HEALTHCARE INFORMATICS (Open Access)

(2021) *ARPN Journal of Engineering and Applied Sciences*, 16 (21), pp. 2264-2274. Cited 2 times.