Documents

Ahmed, F.[a] , Gunawan, T.S.[a] , Nordin, A.N.[a] , Rahim, R.A.[a] , Zain, Z.M.[b] , Zaki Hamidi, E.A.[c]

Deep Learning-Based High Performance Intrusion Detection System for Imbalanced Datasets

(2023) *Proceeding of 2023 9th International Conference on Wireless and Telematics, ICWT 2023*, .

DOI: 10.1109/ICWT58823.2023.10335377

[a] International Islamic Univ. Malaysia, Ece Department, Kuala Lumpur, Malaysia
[b] Universiti Teknologi Mara, Faculty of Applied Science, Shah Alam, Malaysia
[c] Uin Sunan Gunung Djati, Department of Electrical Engineering, Bandung, Indonesia

Abstract
In recent years, the explosive growth in internet and technology use has led to an alarming escalation in both the frequency and severity of cyberattacks. As such, proactive detection and prevention of these attacks have become a matter of paramount importance. This need for vigilance has catalyzed the adoption of Machine Learning (ML) and Deep Learning (DL) techniques to effectively identify and analyze network traffic content, predict potential cyberattacks, and respond promptly to these security threats. ML and DL methods offer innovative solutions by facilitating the development of sophisticated models that meticulously analyze patterns in network traffic data. By identifying deviations from expected behaviors, these techniques enable the early detection and prevention of impending attacks. They achieve this by learning from the data, improving their ability to detect attacks over time, and responding effectively to new, unseen threats. However, contemporary intrusion detection methods face significant challenges, particularly related to imbalanced classes, low detection rates, and high false alarm rates. Addressing these hurdles is critical for the development of a robust and efficient intrusion detection system. Our research seeks to confront these issues head-on, by proposing an innovative, high-performance intrusion detection system tailored specifically to handle imbalanced datasets. Our methodology not only offers improvements in detection rates and false alarm rates but also provides a feasible solution for handling class imbalance in the data. We anticipate that our findings will pave the way for more robust cyber defense mechanisms in this era of ever-evolving security threats. © 2023 IEEE.

Author Keywords
deep learning; feature extraction; imbalanced classes; intrusion detection system

Index Keywords
Alarm systems, Computer crime, Cybersecurity, Deep learning, Errors, Image resolution, Intrusion detection, Learning systems, Network security; Cyber-attacks, Deep learning, Features extraction, Imbalanced class, Imbalanced dataset, Intrusion Detection Systems, Machine-learning, Network traffic, Performance, Security threats; Feature extraction

References

- Yedukondalu, G., Bindu, G.H., Pavan, J., Venkatesh, G., SaiTeja, A.
  Intrusion Detection System Framework Using Machine Learning
  (2021) *The 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA*,
- Phadke, A., Kulkarni, M., Bhawalkar, P., Bhattad, R.
  (2019) *A Review of Machine Learning Methodologies for Network Intrusion Detection*,
- Das, A., Balakrishnan, S.G.
  A Comparative Analysis of Deep Learning Approaches in Intrusion Detection System
  (2021) *The 2021 International Conference on Recent Trends on Electronics*, Information, Communication & Technology RTEICT
- Kishore, R., Chauhan, A.
  (2020) *Intrusion Detection System a Need*,
- Vij, C., Saini, H.
  Intrusion Detection Systems: Conceptual Study and Review
  (2021) *The 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC*,

- Hodo, E.
  (2016) *Threat Analysis of IoT Networks Using Artificial Neural Network Intrusion Detection System*,

- Ashiku, L., Dagli, C.
  (2021) *Network Intrusion Detection System Using Deep Learning*,

- Alhakami, W., Alharbi, A., Bourouis, S., Alroobaea, R., Bouguila, N.
  Network Anomaly Intrusion Detection Using a Nonparametric Bayesian Approach and Feature Selection
  (2019) *IEEE Access*, 7, pp. 52181-52190.

- Mbow, M., Koide, H., Sakurai, K.
  An Intrusion Detection System for Imbalanced Dataset Based on Deep Learning
  (2021) *The 2021 Ninth International Symposium on Computing and Networking (CANDAR*,

- Halimaa, A., Sundarakantham, D.K.
  (2019) *Machine Learning Based Intrusion Detection System*,

- Dhillon, H., Haque, A.
  Towards Network Traffic Monitoring Using Deep Transfer Learning
  (2020) *The 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom*,

- Zheng, X., Wang, Y., Jia, L., Xiong, D., Qiang, J.
  Network Intrusion Detection Model based on Chi-square Test and Stacking Approach
  (2020) *The 2020 7th International Conference on Information Science and Control Engineering (ICISCE*,

- Thaseen, I.S., Kumar, C.A., Ahmad, A.
  Integrated Intrusion Detection Model Using Chi-Square Feature Selection and Ensemble of Classifiers
  (2018) *Arabian Journal for Science and Engineering*, 44 (4), pp. 3357-3368.

- Abouzakhar, N.S., Bakar, A.
  (2010) *A Chi-square Testing-based Intrusion Detection Model*,

- Thaseen, I.S., Kumar, C.A.
  Intrusion Detection Model Using Chi Square Feature Selection and Modified Nave Bayes Classifier
  (2016) *Proceedings of the 3rd International Symposium on Big Data and Cloud Computing Challenges (ISBCC-16*, pp. 81-91.
  Smart Innovation, Systems and Technologies, ch. Chapter 7

- She, X., Sekiya, Y.
  A Convolutional Autoencoder Based Method with SMOTE for Cyber Intrusion Detection
  (2021) *The 2021 IEEE International Conference on Big Data (Big Data*,

Publisher: Institute of Electrical and Electronics Engineers Inc.

Conference name: 9th International Conference on Wireless and Telematics, ICWT 2023
Conference date: 6 July 2023 through 7 July 2023
Conference code: 195291

ISBN: 9798350305029
Language of Original Document: English
Abbreviated Source Title: Proceeding Int. Conf. Wirel. Telemat., ICWT
2-s2.0-85181773411
Document Type: Conference Paper

Publication Stage: Final
Source: Scopus