

Systematic Literature Review: Implementation of Machine Learning for Intrusion Detection

Amanda Amelia Khilda^{✉1}, M. Shaquille Rayhan², Annisa Rizki Amaliah³, Nurbojatmiko⁴

¹Science and Technology, Syarif Hidayatullah State Islamic University Jakarta, Jl. Ir H. Juanda No.95, Tangerang Selatan, 15412, Indonesia, amandaameliakhildaa@gmail.com

²Science and Technology, Syarif Hidayatullah State Islamic University Jakarta, Jl. Ir H. Juanda No.95, Tangerang Selatan, 15412, Indonesia, muhammad_rayhan21@mhs.uinjkt.ac.id

³Science and Technology, Syarif Hidayatullah State Islamic University Jakarta, Jl. Ir H. Juanda No.95, Tangerang Selatan, 15412, Indonesia, annisa.rizki21@mhs.uinjkt.ac.id

⁴Science and Technology, Syarif Hidayatullah State Islamic University Jakarta, Jl. Ir H. Juanda No.95, Tangerang Selatan, 15412, Indonesia, nurbojatmiko@uinjkt.ac.id

✉Corresponding Author: amandaameliakhildaa@gmail.com | Phone: +6285803929763

Received: 07 April 2025

Revision: 22 June 2025

Accepted: 30 August 2025

Abstract

The rapid development of information technology has an impact on the increasing threat to cyber security. One of the main threats is intrusion attacks that are increasingly complex and diverse. To solve this problem, machine learning-based Intrusion Detection System (IDS) is a promising solution due to its ability to detect threats automatically and efficiently. However, the large number of machine learning methods available poses a challenge in determining the best approach for various needs. This research aims to conduct a systematic literature review using PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines. This literature review identifies and categorises previous studies related to the application of machine learning in IDSs based on the problem addressed, proposed solution, research method, metric parameters, research object, and research results. The data for this research is taken from trusted sources, such as Google Scholar, IEEE, Elsevier, Springer, and MDPI. The results of this review are expected to provide a deeper understanding of the application of machine learning in IDS and provide direction for other researchers to fill the remaining research gaps.

Keywords: Cyber Security, Intrusion Detection System, Machine Learning

Introduction

In recent years, the reliance on network-connected devices has increased significantly. This dependency has made device and network security extremely important, fuelling the development of research in the field of cybersecurity. One of the main focuses in this field is finding methods to prevent malicious attacks that can damage organisations, industrial entities, governments, or individual privacy (Daud et al., 2023).

Intrusion Detection System (IDS) is a software or hardware-based system designed to automatically detect intrusions. An intrusion is a suspicious or malicious attempt to access a network (Bace and Mell, 2001; Stavroulakis and Stamp, 2010). In addition to IDS, Intrusion Prevention System (IPS) has the additional capability to prevent detected incidents. Some literature uses the term Intrusion Detection and Prevention System (IDPS) to describe IPS, although this term is rarely used in the cybersecurity community.

There are three main types of IDS, namely Network-based Intrusion Detection System (NIDS), Host-based Intrusion Detection System (HIDS), and Distributed Intrusion Detection System (DIDS). NIDS analyse network traffic to detect attacks or intrusions and are usually deployed in critical network segments. HIDS monitors activity on individual devices, such as servers, to detect attacks. DIDS, as a hybrid of NIDS and HIDS, consists of a collection of IDS sensors that are connected and provide reports to a centralised management system (Ariyus, 2007).

Although network-based IDSs, such as NIDS, have been widely used, conventional techniques still struggle to detect complex attacks, such as zero-day attacks. This has led to the use of machine learning techniques in network anomaly detection. These techniques allow computers to learn from previous data and predict the status of new data. Various machine learning models have their own advantages, which make them suitable for certain situations (Hamid, Sugumaran, & Journaux, 2016).

This research aims to review the literature on the application of machine learning in IDS, especially in anomaly-based IDS. It analyses the models and methodologies used in various studies to find the most effective approach. The research also compares the performance of several machine learning models based on their effectiveness in detecting threats.

To solve the problems described, this research uses the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) method. This method involves the stages of systematic search, selection, and evaluation of literature to ensure the accuracy and relevance of the research. With the PRISMA method, this research aims to provide a comprehensive view of the application of machine learning in IDS as well as filling the gaps in previous research.

Literature Review

Research in the field of Intrusion Detection System (IDS) continues to grow to address increasingly complex and diverse network threats. IDS has several approaches, including Network-based Intrusion Detection System (NIDS) and Host-based Intrusion Detection System (HIDS). In addition, detection techniques in IDS are also evolving, such as signature-based detection and anomaly-based detection approaches.

A study compared machine learning (ML) and deep learning (DL) models used in anomaly-based intrusion detection systems. This research provided an overview of previously used models and datasets such as KDD-99 were tested to measure model performance (Abdel-Wahab, Neil, & Atia, 2020). The results showed that while no model was considered overall superior, the Random Forest (RF) model showed promising results and deserves further testing in real-world scenarios. This research also highlighted the need for the development of online learning techniques and dataset updates to be more relevant to modern network attacks.

Another study developed a distributed intrusion detection system (DIDS) architecture by utilising cloud computing and blockchain infrastructure (Kumar & Singh, 2020). The researchers tested the performance of DIDS under various data loads, and analysed issues such as communication delay, overhead of blockchain, and implementation cost. The results showed that the integration of these new technologies has the potential to significantly improve network security.

Furthermore, a study demonstrated a security infrastructure for vehicle information that combines Software Defined Networking (SDN), intrusion detection, and a cloud-based defence centre. This infrastructure improves protection, monitoring, detection, incident management, and response to threats attacking vehicles and fleets (Meyer et al., 2020). The results of this study emphasise the importance of technology integration to create a security system that is responsive to various threats in the vehicle environment.

Another study proposed a deep learning-based attack detection method to improve data security in social networks (Jiang et al., 2020). This research combines data preprocessing, feature extraction, and multi-channel training using Long Short-Term Memory Recurrent Neural Networks (LSTM-RNN). By using a voting algorithm to determine whether the input data is an attack, the method achieves high accuracy in detecting threats.

The latest research investigates improving IDS performance through an early detection approach in local area networks using industrial control systems and honeypots (Pashaei et al., 2020). The researchers simulated DDoS attacks and port scanners on various operating systems and devices. The results show that the designed IDS can detect simulated attacks in less than one second with a detection probability of 78%. This research emphasises the importance of integration between honeypots and IDS to improve intrusion detection efficiency in industrial environments.

Materials & Methods

The method used in this study was a literature study with PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines to ensure transparency, repeatability, and scientific rigour. Stages included the development of a review protocol, explanation of article selection criteria, search strategy, data extraction, and data analysis procedures. This approach is designed to minimise bias and increase the validity of research results through structured and systematic steps (Georgopoulos et al., 2023).

Research Question

Formulating Research Questions (RQ) as the main guide in conducting literature review, the following research questions were formulated:

RQ1: What are the most commonly used machine learning algorithms in intrusion detection systems, and how does each algorithm perform based on studies that have been conducted?

RQ2: What factors affect the effectiveness of machine learning implementation in intrusion detection, such as dataset type and performance measurement method?

Eligibility Criteria

The following Inclusion Criteria (IC) were set to guide this literature review:

IC1: The years of articles used are only the last 5 years, namely 2018-2024.

IC2: The topic of the article used is Machine Learning for Intrusion Detection.

IC3: The article must be original research that has been reviewed and written in English.

Data Sources

This research uses various sources of information, including scientific databases such as Google Scholar, IEEE Xplore, ScienceDirect, Elsevier, Springer, and MDPI. These sources formed the main basis of data collection for this research. During the research process, articles that were not fully accessible to the authors were removed. In addition, a scan of the reference lists in the articles was conducted to find related studies, as well as a reference search in the list of articles that met the inclusion criteria to look for other possible relevant related studies. The search results using predefined keywords yielded more than twelve thousand articles. Then, articles that did not meet the inclusion criteria were removed, and finally, the top 30 articles were selected for further review.

Study Selection

Study selection was conducted through the following four stages:

a. Keyword Determination

Determining relevant keywords for the article search, which included terms such as 'machine learning' 'intrusion detection' and other related words. The selection of these keywords was based on the scope of the two research

questions that had been formulated.

- b. Exploration and Selection of Titles, Abstracts, and Keywords
Using the predetermined keywords, relevant scientific article sources were explored. Then, the titles, abstracts, and keywords of the articles found were evaluated and selected based on the predetermined eligibility criteria.
- c. Full or Partial Reading of Articles
Articles that pass the previous stage are read in full or in part to assess the extent to which the article is relevant and whether it meets the predetermined eligibility criteria. Articles that do not fulfil the criteria are removed from the study.
- d. Reference List Review
The reference lists of the selected articles were reviewed. The aim is to find other relevant studies that may not have been included in the initial search. References from selected articles will be analysed to ensure completeness and inclusiveness in addressing the use of semantic technologies in enterprise knowledge management.

Data Analysis

Data was extracted from the 30 selected literatures by categorising them based on problems, solutions, research methods, objects, and research results. The categorised data was then visualised using diagrams created with the help of Excel software. In addition, a comparative analysis was also conducted on articles that used experimental methods in their research to compare the results and approaches used in more depth. This approach aims to provide a comprehensive overview of relevant research trends and findings.

Results and Discussion

By using a literature review using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) method, this research produces various important findings related to the application of machine learning techniques for intrusion detection. Researchers conducted a systematic literature review to compare various machine learning algorithms or techniques used in detecting suspicious activity or attacks on computer systems or networks. Intrusion Detection System is designed to protect system security by identifying, analysing, and reporting unusual activities. More than 12,000 articles were found through the search. After removing duplicates and filtering by title and abstract, 30 papers that met the inclusion criteria were selected for in-depth analysis in full text.

Research Question

RQ1: What are the most commonly used machine learning algorithms in intrusion detection systems, and how do they perform based on the studies that have been conducted?

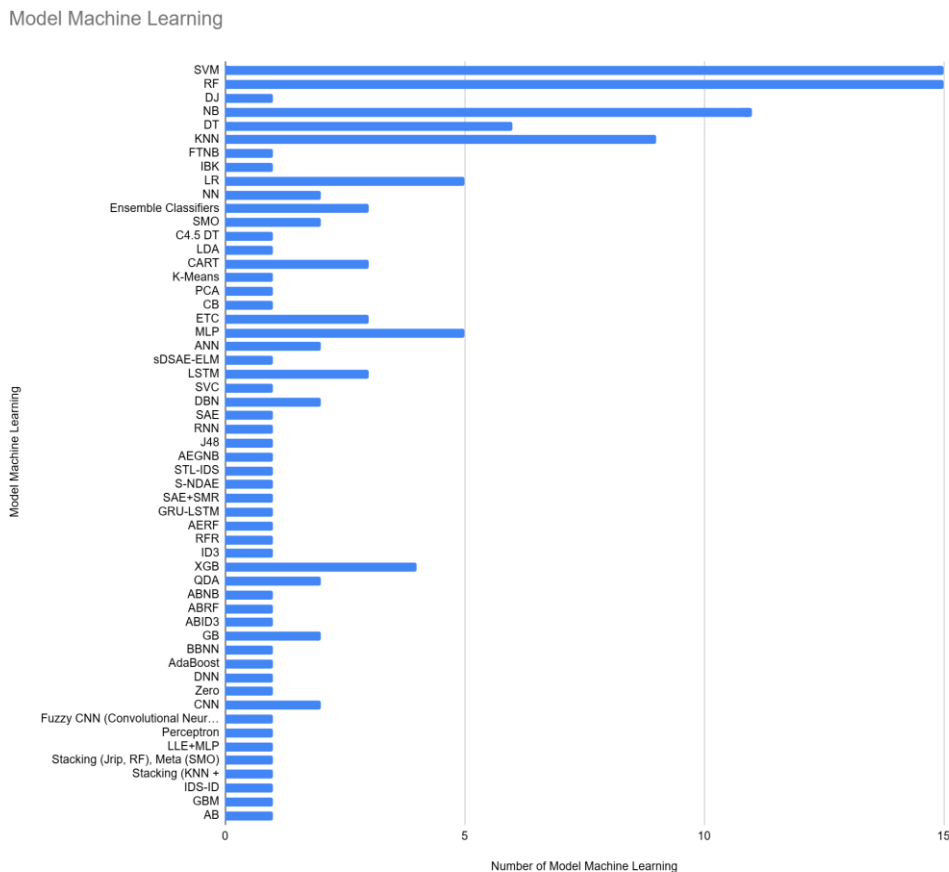


Figure 1. Machine Learning Models that are Often used in Research

Seen in Figure 1. is the use of Machine Learning methods that are often used in a study. SVM (Support Vector Machine) is the most frequently used model, with close to or equal to 15 times. Models such as NB (Naïve Bayes) and FTNB are also used quite frequently as well, and other models such as C4.5 DT, ETC, and XGB have a lower usage rate, around 5 times or less. Some models, such as Perceptron and Stacking (KNN + AB), were seen to be used very rarely.

The SVM method is often used in IDS research due to its ability to handle imbalanced data, work effectively on high-dimensional datasets, and have good generalisability. SVM also excels in classifying non-linear data using kernels, is resistant to noise, and is able to detect attacks quickly and accurately, including new attack patterns. The flexibility in kernel selection and success in various studies make it a popular choice, although it requires proper parameter tuning for optimal performance.

Best Model Machine Learning

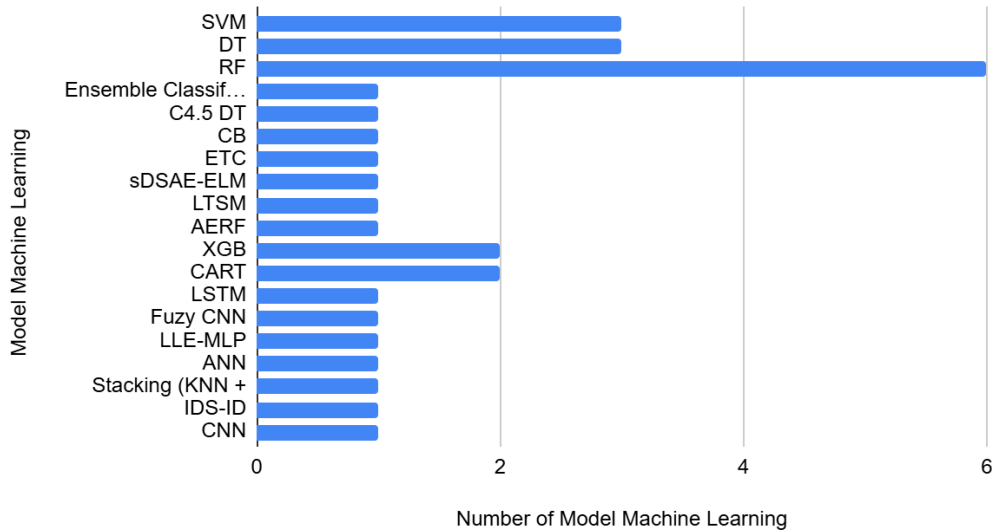


Figure 2. The Best Machine Learning Model Based on Research Results

Figure 2. displays a graph showing the best machine learning models based on the research results. Rain Forest (RF) stands out as the most frequently considered best model, with the highest number of uses being around 6 times. Other models such as SVM (Support Vector Machine) and DT (Decision Tree) were also used quite frequently, with a frequency of about 2-3 times. Some other models, such as XGB (XGBoost), and Classification and Regression Trees (CART), had lower frequencies, indicating that they were considered best in certain contexts. This reflects that Rain Forest has a superior ability to combine different models to improve accuracy, while other models are selected according to the specific needs and data type of the study.

RQ 2: What factors influence the effectiveness of applying machine learning to intrusion detection, such as dataset type and performance metrics?

Count of Dataset

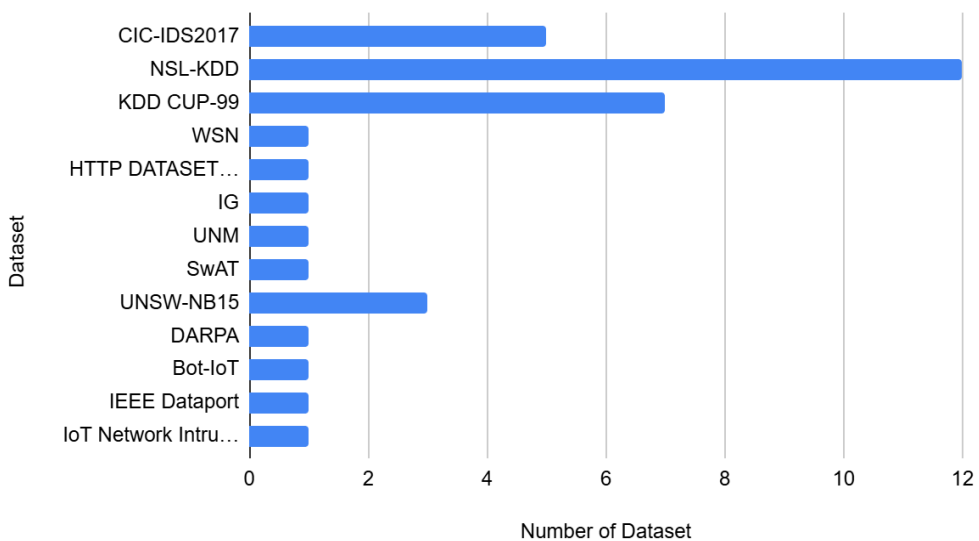


Figure 3. Datasets Often used in Research

Figure 3 shows the various datasets that are often used in machine learning-based intrusion detection research. The NSL-KDD dataset is the most dominant with the highest number of uses, which is 12 times. This shows that NSL-KDD is still the main reference for researchers because this dataset offers more structured data than its predecessor, KDD CUP-99, and eliminates redundant data. In addition, KDD CUP-99, which was used 7 times, is still quite popular because many older studies used it, so modern researchers tend to use it for comparison of results.

Other datasets such as CIC-IDS2017 were used 5 times and are starting to become an option as they cover more recent and complex attack data. CIC-IDS2017 represents modern attack scenarios, making it a relevant alternative for research in this area. UNSW-NB15 also attracted attention with a usage count of 3 times, indicating an interest in datasets that cover more features and attack variations than other datasets.

Several other datasets such as WSN, DARPA, Bot-IoT, and SwAT had relatively low usage of 1 to 2 times. This shows that the research focus still tends to use more conventional or general datasets rather than specific datasets such as those related to IoT and critical systems. However, the existence of these datasets shows that intrusion detection research is starting to expand into new, more specific areas, such as IoT and critical infrastructure security.

The diversity of datasets used in this research reflects the pressing need to explore a wide range of attack scenarios that cover different types of network security threats. Although the NSL-KDD dataset still dominates as the first choice for many researchers due to its simplicity and relevance to previous research, there is an increasingly strong trend that shows a growing interest in starting to move towards newer datasets. These datasets offer more complex data coverage and are relevant to modern network security challenges, including emerging threats due to technological evolution and increasingly sophisticated cyber attack patterns.

Count of Performance Metrics

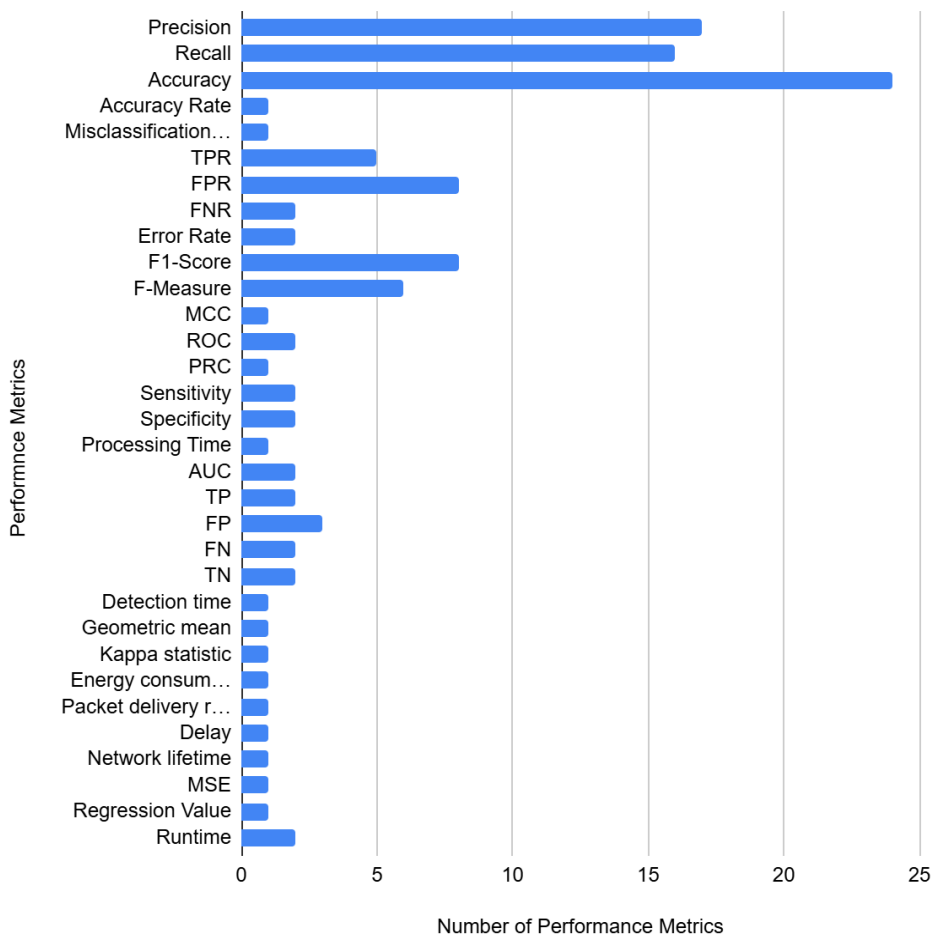


Figure 4. Measurement Metrics that are Often Tested in Research

Figure 4 shows the performance metrics used in machine learning research for intrusion detection. From the graph, it can be seen that accuracy is the most frequently used metric, with the highest number of uses, which is 24 times. This shows that researchers still prioritise accuracy as the main measure of the model's success in classifying data. In addition, precision and recall also occupy a high position, used 17 and 16 times respectively. These two metrics are very important because precision measures how good the model is at avoiding false positives, while recall assesses the model's ability to consistently detect attacks without missing threats.

In addition to these three main metrics, other metrics, such as F-Measure were used 6 times, indicating that researchers are increasingly aware of the need to evaluate the balance between precision and recall, especially in cases where the dataset has an unbalanced class distribution. FPR (False Positive Rate) and F1-Score were also frequently used, 8 times each, as indicators to measure the model's error rate in predicting both attack and normal data. This is important in ensuring that the system does not generate too many false alarms that can interfere with decision making.

There was use of other metrics such as TPR, Sensitivity, and Specificity, which were used 2 to 5 times each. These metrics are relevant in certain contexts, for example to evaluate model performance on real-time systems or high-risk scenarios. In addition, more technical metrics such as MCC, AUC, and ROC indicate an interest in more mathematical and holistic model evaluation, although they are still used relatively infrequently compared to key metrics such as accuracy and precision. Some metrics such as energy consumption, delay, and runtime, were used 1 to 2 times. Although less popular, these metrics are important in efficiency-focused research, such as IoT-based systems or resource-constrained networks. Overall, this graph reflects that while accuracy, precision, and recall are the main focus, researchers also consider various metrics to evaluate machine learning models in more specific scenarios.

Conclusions

This research successfully provides a systematic literature review on the application of machine learning in Intrusion Detection System (IDS). Using the PRISMA method, this research identifies frequently used machine learning algorithms, such as Support Vector Machine (SVM) and Random Forest (RF), which are proven effective in detecting network threats. The analysis results show that SVM excels in handling high-dimensional and non-linear data, while RF stands out in combining models to improve detection accuracy. In addition, this research highlights the importance of using cutting-edge datasets, such as CIC-IDS2017, which reflect modern attack patterns. However, the review also revealed research gaps, such as the lack of online learning techniques and the need for dataset updates to deal with increasingly complex threats. This research emphasises the need to develop machine learning-based IDSs that are adaptive and responsive to various attack scenarios. In terms of performance evaluation, metrics such as accuracy, precision and recall are still the main focus, although future research needs to consider additional metrics such as energy consumption and runtime for applications on resource-constrained devices. With a comprehensive approach, this research is expected to serve as a reference for the development of more innovative and effective IDSs. Therefore, collaboration between researchers and practitioners is expected to accelerate the implementation of machine learning-based IDS solutions to improve network security.

References

- Abdallah, E. E., Eleisah, W., & Otoom, A. F. (2022). Intrusion Detection Systems Using Supervised Machine Learning Techniques: A Survey. *Procedia Computer Science*, 201, 205–212. <https://doi.org/10.1016/j.procs.2022.03.029>
- Abdel-Wahab, M. S., Neil, A. M., & Atia, A. (2020). A Comparative Study Of Machine Learning And Deep Learning In Network Anomaly-Based Intrusion Detection Systems. In *Proceedings Of The 15th International Conference On Computer Engineering And Systems (Icces)*, 1–6. <https://doi.org/10.1109/icces51560.2020.9334553>
- Abrar, I., Ayub, Z., Masoodi, F., & Bamhdi, A. M. (2020). A Machine Learning Approach For Intrusion Detection System On Nsl-Kdd Dataset. In *Proceedings Of The 2020 International Conference On Smart Electronics And Communication (Icosec)*, 919–924. <https://doi.org/10.1109/icosec49089.2020.9215232>
- Ahmad, A. Et Al. (2020). Machine Learning-Based Distributed Denial Of Service Attack Detection On Intrusion Detection System Regarding To Feature Selection. *International Journal Of Artificial Intelligence Research*, 4(1), 1-8. <https://doi.org/10.29099ijair.v4i1.156>.
- Ahmed, L. A. H., & Hamad, Y. A. M. (2021). Machine Learning Techniques For Network-Based Intrusion Detection System: A Survey Paper. In *Proceedings Of The 2021 National Computing Colleges Conference (Nccc)*, 1–7. <https://doi.org/10.1109/nccc49330.2021.9428827>
- Alsahli, M. S., Almasri, M. M., Al-Akhras, M., Al-Issa, A. I., & Alawairdhi, M. (2021). Evaluation Of Machine Learning Algorithms For Intrusion Detection System In Wsn. *International Journal Of Advanced Computer Science And Applications (Ijacs)*, 12(5). <http://dx.doi.org/10.14569/ijacs.2021.0120574>
- Ariyus, D. (2007). Intrusion Detection System. *Andi*.
- Azizan, A. H., Mostafa, S. A., Mustapha, A., Foozy, C. F. M., Wahab, M. H. A., Mohammed, M. A., & Khalaf, B. A. (2021). A Machine Learning Approach For Improving The Performance Of Network Intrusion Detection Systems. *Annals Of Emerging Technologies In Computing (Aetic)*, 5(5), 201-208. <https://doi.org/10.33166/aetic.2021.05.025>.
- Bace, R., & Mell, P. (2001). Intrusion Detection Systems (Technical Report 800-31). *National Institute Of Standards And Technology (Nist)*.
- Baci, N., Vukatana, K., & Baci, M. (2022). Machine Learning Approach For Intrusion Detection Systems As A Cyber Security Strategy For Small And Medium Enterprises. *Wseas Transactions On Business And Economics*, 19, 474-480. <https://doi.org/10.37394/23207.2022.19.43>
- Cheng, X., Li, W., Xiao, Z., & Zhao, T. (2020). Intrusion Detection System Based On Qbso-Fs. In *Proceedings Of The 2020 International Conference On Artificial Intelligence And Computer Engineering (Icaice)*, 372–377. <https://doi.org/10.1109/icaice51518.2020.00078>
- Daud, M., Zulfikar, M. Y., Hasibuan, A., & Isa, M. (2023). Prototype Of Automatic Watering And Fertilizing System For Oil Palm Seeds Based On Internet Of Things. *Andalas Journal Of Electrical And Electronic Engineering Technology*, 3(1), 1–9.

- Das, S., Ashrafuzzaman, M., Sheldon, F. T., & Shiva, S. (2020). Network Intrusion Detection Using Natural Language Processing And Ensemble Machine Learning. In *Proceedings Of The 2020 Ieee Symposium Series On Computational Intelligence (Ssci)*, 829–835. <https://doi.org/10.1109/ssci47803.2020.9308268>
- Halimaa, A., & Sundarakantham, K. (2019). Machine Learning Based Intrusion Detection System. In *Proceedings Of The 2019 3rd International Conference On Trends In Electronics And Informatics (Icoei)*, 916–920. <https://doi.org/10.1109/Icoei.2019.8862784>
- Hamid, Y., Sugumaran, M., & Journaux, L. (2016). Machine Learning Techniques For Intrusion Detection: A Comparative Analysis. In *Proceedings Of The International Conference On Informatics And Analytics (Icia-16)*. Association For Computing Machinery. <https://doi.org/10.1145/2980258.2980378>
- Hassan, E. M., Saleh, M. A., & Ahmed, A. M. (2020). Network Intrusion Detection Approach Using Machine Learning Based On Decision Tree Algorithm. *Journal Of Engineering And Applied Sciences-Je&As*, 7(2), 1-1. <https://doi.org/10.5455/jeas.2020110101>
- Isa, M. M., & Mhamdi, L. (2020). Native Sdn Intrusion Detection Using Machine Learning. In *Proceedings Of The 2020 Ieee Eighth International Conference On Communications And Networking (Comnet)*, 1–7. <https://doi.org/10.1109/comnet47917.2020.9306093>
- Jiang, F., Et Al. (2020). Deep Learning Based Multi-Channel Intelligent Attack Detection For Data Security. *Ieee Transactions On Sustainable Computing*, 5(2), 204–212. <https://doi.org/10.1109/Tsusc.2018.2793284>
- Kavitha, G., & Elango, N. M. (2020). An Approach To Feature Selection In Intrusion Detection Systems Using Machine Learning Algorithms. *International Journal Of E-Collaboration (Ijec)*, 16(4), 48-58. <https://doi.org/10.4018/ijec.2020100104>
- Kumar, M., & Singh, A. K. (2020). Distributed Intrusion Detection System Using Blockchain And Cloud Computing Infrastructure. In *Proceedings Of The 4th International Conference On Trends In Electronics And Informatics (Icoei)*, 248–252. <https://doi.org/10.1109/icoei48184.2020.9142954>
- Kumar, S. V. N., Selvi, M., Kannan, A., & Doulamis, A. D. (2023). A Comprehensive Survey On Machine Learning-Based Intrusion Detection Systems For Secure Communication In The Internet Of Things. *Intelligent Neuroscience*, 2023, 1–17. <https://doi.org/10.1155/2023/8981988>
- Liu, Z., Thapa, N., Shaver, A., Roy, K., Yuan, X., & Khorsandroo, S. (2020). Anomaly Detection On Iot Network Intrusion Using Machine Learning. In *Proceedings Of The 2020 International Conference On Artificial Intelligence, Big Data, Computing And Data Communication Systems (Icabcd)*, 1–5. <https://doi.org/10.1109/icabcd49160.2020.9183842>
- Meyer, P., Et Al. (2020). Demo: A Security Infrastructure For Vehicular Information Using Sdn, Intrusion Detection, And A Defense Center In The Cloud. In *Proceedings Of The 2020 Ieee Vehicular Networking Conference (Vnc)*, 1–2. <https://doi.org/10.1109/vnc51378.2020.9318351>
- Mishra, P., Varadharajan, V., Pilli, E. S., & Tupakula, U. (2020). Vmguard: A Vmi-Based Security Architecture For Intrusion Detection In Cloud Environment. *Ieee Transactions On Cloud Computing*, 8(3), 957–971. <https://doi.org/10.1109/tcc.2018.2829202>
- Musaab R., Dina A.. (2021). Intrusion Detection System Based On Machine Learning Techniques. *Indonesian Journal Of Electrical Engineering And Computer Science*, Vol. 23, No. 2, Pp. 953-961, <https://doi.org/10.11591/ijeecs.v23.i2.pp953-961>
- Musleh, D., Alotaibi, M., Al-Haidari, F., Rahman, A., & Mohammad, R. (2023). Intrusion Detection System Using Feature Extraction With Machine Learning Algorithms In Iot. *Journal Of Sensor And Actuator Networks*, 12, 1-19. <https://doi.org/10.3390/jsan12020029>
- Nerlikar P., Pandey S., Sharma S., And Bagade S. (2020). Analysis of Intrusion Detection Using Machine Learning Techniques. *Int. J. Comput. Netw. Commun. Secur.*, Vol. 8, No. 10, Pp. 84–93
- Pallepati, M., Voggu, S., Masula, R., & Konjarla, M. (2022). Network Intrusion Detection System Using Machine Learning With Data Preprocessing And Feature Extraction. *International Journal For Research In Applied Science And Engineering Technology*, 10, 2360-2365. <https://doi.org/10.22214/ijraset.2022.44326>
- Parashar, A., Saggu, K. S., & Garg, A. (2022). Machine Learning Based Framework For Network Intrusion Detection System Using Stacking Ensemble Technique. *Indian Journal Of Engineering And Materials Sciences (Ijems)*, 29(4), 509-518. <https://doi.org/10.56042/ijems.v29i4.46838>
- Pashaei, A., Akbari, M. E., Lighvan, M. Z., & Teymorzade, H. A. (2020). Improving The Ids Performance Through Early Detection Approach In Local Area Networks Using Industrial Control Systems Of Honeypot. In *Proceedings Of The 2020 Ieee International Conference On Environment And Electrical Engineering And 2020 Ieee Industrial And Commercial Power Systems Europe (Eeeic / I&Cps Europe)*, 1–5. <https://doi.org/10.1109/eeic/icpsueurope49358.2020.9160574>
- Pordelkhaki, M., Fouad, S., & Josephs, M. (2021, November). Intrusion Detection For Industrial Control Systems By Machine Learning Using Privileged Information. In *2021 Ieee International Conference On Intelligence And Security Informatics (Isi)* (Pp. 1-6). <http://doi.org/10.1109/isi53945.2021.9624757>
- Purbo, W. O. (2006). *Buku Pinter Internet Tcp/lp*. Pt. Elex Media Komputindo.
- Saranya, T., Sridevi, S., Deisy, C., Chung, T. D., & Khan, M. K. A. A. (2020). Performance Analysis Of Machine Learning Algorithms In Intrusion Detection System: A Review. *Procedia Computer Science*, 171, 1251–1260. <https://doi.org/10.1016/j.procs.2020.04.133>
- Singhal, A., Maan, A., Chaudhary, D., & Vishwakarma, D. (2021). A Hybrid Machine Learning And Data Mining Based

- Approach To Network Intrusion Detection. In *Proceedings Of The 2021 International Conference On Artificial Intelligence And Smart Systems (Icais)*, 312–318. <https://doi.org/10.1109/icaais50930.2021.9395918>
- Stavroulakis, P., & Stamp, M. (2010). *Handbook Of Information And Communication Security*. Springer-Verlag.
- Swarna Sugi, S. S., & Ratna, S. R. (2020). Investigation Of Machine Learning Techniques In Intrusion Detection System For Iot Network. In *Proceedings Of The 2020 3rd International Conference On Intelligent Sustainable Systems (Iciss)*, 1164–1167. <https://doi.org/10.1109/iciss49785.2020.9315900>
- Thapa, N., Liu, Z., Kc, D. B., Gokaraju, B., & Roy, K. (2020). Comparison Of Machine Learning And Deep Learning Models For Network Intrusion Detection Systems. *Future Internet*, 12(10), 167. <https://doi.org/10.3390/Fi12100167>
- Umer, M. A., Junejo, K. N., Jilani, M. T., & Mathur, A. P. (2022). Machine Learning For Intrusion Detection In Industrial Control Systems: Applications, Challenges, And Recommendations. *International Journal Of Critical Infrastructure Protection*, 38, 100516. <https://doi.org/10.1016/j.ijcip.2022.100516>
- Verma, A., & Ranga, V. (2023). Machine Learning Based Intrusion Detection Systems For Iot Applications. <https://doi.org/10.48550/arxiv.2302.12452>
- Zhang, G., Wang, X., Li, R., Lai, J., Xiang, Q., & He, J. (2020). Network Intrusion Detection Method Based On Stacked Denoising Sparse Autoencoder And Extreme Learning Machine. In *Proceedings Of The 2020 2nd International Conference On Information Technology And Computer Application (Itca)*, 194–199. <https://doi.org/10.1109/itca52113.2020.00048>
- Zhang, L., Kuang, X., Xu, A., Suo, S., & Yang, Y. (2020). A Novel Network Intrusion Detection System Based On Cnn. In *Proceedings Of The 2020 Eighth International Conference On Advanced Cloud And Big Data (Cbd)*, 243–247. <https://doi.org/10.1109/cbd51900.2020.00051>