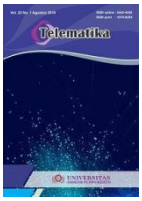

Available online at :
http://ejournal.amikompurwokerto.ac.id/index.php/telematika/

Telematika

Accreditated SINTA "2" Kemenristek/BRIN, No. 85/M/KPT/2020

Systematic Review of Supervised Learning Models for Network Flood Detection (NFD): Trends, Performance Evaluation, and Implementation Insights

Roni Habibi[1], Naufal Dekha Widana[2]

[1,2] Universitas Logistik dan Bisnis Internasional,

ARTICLE INFO

History of the article:
Received April 5, 2025
Revised May 10, 2025
Accepted August 27, 2025

Keywords:
Network
Machine learning
SLR
DDoS
Supervised Learning

Correspondence:

E-mail: roni.habibi@ulbi.ac.id

ABSTRACT

Due to the growing volume, speed, and sophistication of malicious traffic, Network Flood Detection (NFD), especially in the context of Distributed Denial of Service (DDoS) assaults, continues to be a crucial challenge in contemporary network security. Supervised machine learning has been widely used to enhance the precision, scalability, and real-time detection capabilities of NFD systems. However, current research reveals inconsistent results on the optimal supervised learning algorithm, mostly because of differences in datasets, feature engineering methods, assessment criteria, and deployment settings. In order to assess supervised learning models applied to NFD, this study intends to do a Systematic Literature Review (SLR) utilizing the PRISMA framework. A structured search was performed via Scopus, IEEE Xplore, SpringerLink, and ScienceDirect, encompassing papers from 2019 to 2025. 40 primary papers and 16 additional articles were found to be appropriate for synthesis after an initial dataset of 516 research was reviewed using predetermined inclusion and exclusion criteria. Algorithms, datasets, evaluation criteria, feature selection techniques, and deployment characteristics were all incorporated in the data extraction process. According to the review, models like Random Forest, XGBoost, K-Nearest Neighbor, and Support Vector Machine regularly perform well, with accuracy ranging from 92% to 99%, depending on preprocessing methods and dataset features. Common problems highlighted include dataset imbalance, lack of real-time adaptation, and insufficient generalization to unforeseen assault types. The results show that supervised learning is still a promising method for NFD, particularly when combined with balanced datasets, hybrid or ensemble model techniques, and optimized feature engineering. To increase real-time resilience against changing network threats, further research is urged to incorporate deep learning, lightweight edge models, and adaptive learning frameworks.

1. INTRODUCTION

In contemporary digital ecosystems, service availability and resilience are crucial due to the quick expansion of digital infrastructure and the growing reliance on networked systems (AlShaikh et al. 2025). Because their activities depend on constant and reliable connectivity, critical industries like finance, healthcare, government, and industrial systems are particularly susceptible to network disruptions and security breaches (Shajari et al. 2022). Cyber threats, especially Distributed Denial of Service (DDoS) and Network Flood Attacks, have grown in size, frequency, and complexity as digital services proliferate. If left unchecked, these threats can result in system failure, operational delays, and service degradation (Shajari et al. 2022).

Due to their dependence on pre-established attack patterns, which restricts their capacity to identify unnoticed or altered attacks, traditional intrusion detection techniques, such as rule-based and

signature-based detection, are becoming less and less effective (Zhang 2022). Supervised machine learning, which can learn behavioral patterns from labeled data and improve detection performance beyond static techniques, has emerged as a promising way to overcome this restriction (Altayef et al. 2022). A number of algorithms, including Random Forest (RF), K-Nearest Neighbor (KNN), and Support Vector Machine (SVM), have shown a high degree of classification capacity in differentiating between malicious flood activity and benign traffic (Ndichu et al. 2023). Convolutional neural networks (CNN) and recurrent neural networks (RNN), which offer possible enhancements through automated feature extraction and temporal pattern learning, are also explored by more contemporary frameworks (Z. Wang et al. 2025).Because of differences in dataset features, preprocessing pipelines, feature selection procedures, traffic patterns, and assessment measures, results across studies continue to be inconsistent despite the growing corpus of research (Radhika et al. 2023). Furthermore, current assessments typically blend supervised and unsupervised learning, concentrate on general intrusion detection, or lack a thorough comparative analysis that particularly addresses Network Flood Detection (NFD) (Halder et al. 2024). This raises questions about the best supervised learning strategy for NFD implementations in similar experimental settings.

This study uses the PRISMA approach to conduct a Systematic Literature Review (SLR) based on research published between 2020 and 2025 in order to close this gap (Yi and Tian 2024). Finding pertinent traffic features, assessing detection performance across supervised learning models, and identifying the algorithms with the best stability and usefulness for NFD are the objectives of this study. The results are anticipated to support real-world deployment considerations for machine learning-based NFD systems as well as scholarly research paths.

Therefore, this study conducts a Systematic Literature Review (SLR) using the PRISMA methodology to evaluate supervised learning models applied to NFD. The objectives of this review are to:

RQ : what features are relevant and will greatly influence the performance of NFD?

Through this structured review, the findings aim to support future researchers and practitioners in developing more reliable, scalable, and real-time detection systems capable of mitigating evolving flood-based cyber threats.

2. RESEARCH METHODS

To guarantee methodological transparency and repeatability, the PRISMA systematic review process was followed while choosing the literature for this investigation (Fatriansyah et al. 2023). The Scopus database was chosen for the search procedure because of its broad indexing coverage in the fields of machine learning, networking, and cybersecurity research (Sangodoyin et al. 2021). To maximize relevance, a number of keyword combinations and Boolean operators were employed during the search process, such as "Network Flood With Machine Learning," "Network Flood Detection Device," "DDoS Detection Device," "DDoS Machine Learning Detection," and "Network Anomaly Detection with Machine Learning" (Puttinaovarat and Horkaew 2020). A total of 516 records were found in this first search as shown in figure 1.

Duplicate publications (n = 139) and ineligible records found by automated filters, such as publication year restrictions (2020–2025) (n = 48), were eliminated during the screening step (S. Wang et al. 2021). A smaller dataset of 296 articles was used for first screening after additional exclusions were applied to research that did not fit scope criteria, such as non-Supervised Learning models, non-flood anomaly detection, or non-cybersecurity focus (Kamamura et al. 2023). Following abstract and metadata verification, 178 records were eliminated at this point because they were either irrelevant or did not sufficiently correspond with the research aim (Çevik and Akleylek 2024). 118 records in all underwent full-text eligibility evaluation. Nevertheless, 80 papers were omitted because they could not be retrieved in full text because of access restrictions (Kumar and Gupta 2025). In order to prevent bias or duplication, the same eligibility screening criteria were used to the 16 supplementary records that were obtained from additional pertinent studies that were found outside of the automated search procedure. 40 articles were chosen for assessment after the final inclusion stage, and 56 documented examples of experimental datasets, models, and evaluation metrics served as the foundation for synthesis and comparative analysis (Ullah and Mahmoud 2021).

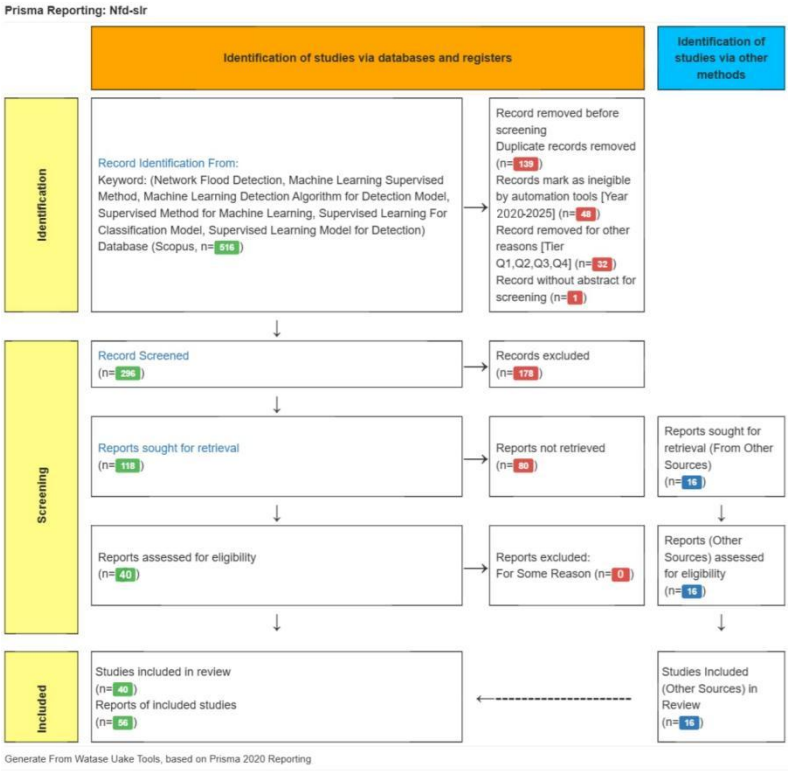

Figure 1. PRISMA Method Table

3. RESULT AND DISCUSSION

3.1. Classification of Publication Year

A variable but significant trend in research interest in supervised learning applications in machine-learning-based detection systems may be seen in the distribution of publications in figure 2 from 2020 to 2025 (F. Wang and Feng 2025). The number of publications started off slowly in 2020 and 2021, suggesting that supervised learning methods were adopted and investigated early in network-based detection research (Patel, B, and Annavarapu 2025). A significant rise in 2022 and a peak in 2023 were indicative of greater attention from academia and industry, probably due to the development of machine learning models and the growing urgency of cybersecurity-related applications [CIT21].

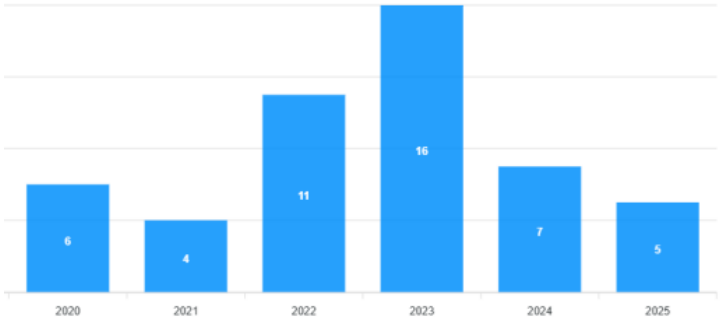

Figure 2. Classification of Publication Year Chart

The frequency of publications decreased after 2023, and fewer research were published in 2024 and the first part of 2025. This decrease may be a sign of a move toward investigating different strategies like deep learning, hybrid intrusion detection models, or anomaly-based detection frameworks rather than a sign of losing relevance (Popoola et al. 2023). The general trend indicates that supervised learning research is still important, but the field has developed, and future research may place more emphasis on optimization, practical application, and comparative analysis than on fundamental investigation (Shaik, Unni, and Zeng 2022).

3.2. Country Classification of Research Authors

Based on figure 3 the graph of the research author's country, Australia, Southeast Asia: This is the group with the largest contribution, with a percentage of 10%, which shows great interest in the application of supervised methods in this region. China: With a sizable contribution from the three components, 10% and 5% respectively, (total 20%), China is the main player in this research. India (including India from Stocktwits from January): Showed significant, albeit low, participation with a 5% contribution.

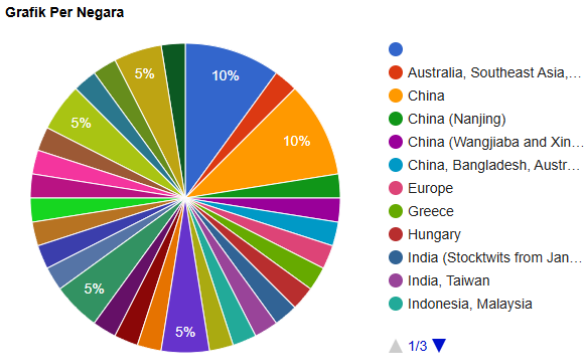

Figure 3. Country Classification of Research Authors Graphic

European countries, Greece and Hungary: each accounted for 5%, showing interest. Indonesia and Malaysia: Shows 5% contribution. This shows that Southeast Asia is involved in research on this topic. This graph shows that China and Australia, along with Southeast Asia, play a dominant role in publishing research related to machine teaching supervision methods. China dominates much of the chart. Malaysia, European countries and Indonesia also contributed, although in smaller amounts.

3.3. Classification Based on research methods

Based on figure 4, which depicts the distribution of research methods, many approaches used for machine learning can be seen. There are several important points that can be concluded about the application of supervised learning methods to various algorithms. AI/ML Model Development (Blue): This graph shows that most research focuses on developing models based on artificial intelligence and machine learning. This may include supervised learning algorithms such as Support Vector Machines (SVM), Decision Trees, and others commonly used in regression or classification problems(Khalid et al. 2019). Logistic Regression (dark green): This graph shows a logistic regressive model for a binary classification problem. This is a conventional method for supervised learning that is often used for predictive analysis. Hybrid Models (orange and purple): Many studies use hybrid models for supervised and unsupervised learning(Park and Choi 2020).

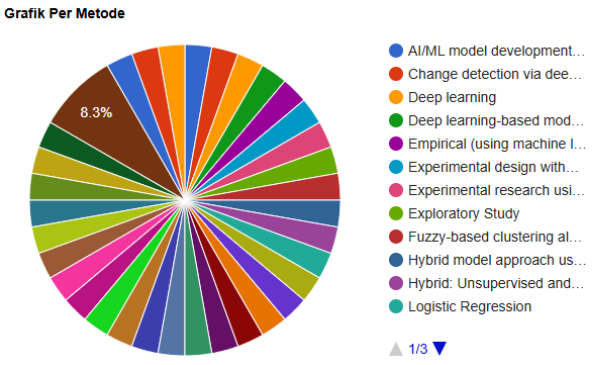

Figure 4. Classification Based on research methods Graphic

This suggests that improving model performance for certain tasks, such as supervised teaching, may become more general by combining multiple models or algorithms. Deep Learning (Red and light blue): This graph shows the use of deep learning, which is often associated with supervised learning. Deep teaching algorithms such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) are often used in supervised teaching, especially for pattern recognition and sequential data analysis problems(Lu et al. 2020). Fuzzy-based Clustering (Greenish): Some studies may use fuzzy approaches to

model data in the context of supervised learning, especially in classification. This is because clustering is more often associated with unsupervised learning. Experiments and Experimental Design (Yellow and blue): This shows that many studies use controlled experiments to test how effective various algorithms, including supervised learning, are in real applications(Birant 2023).

4. WORDCLOUD METADATA KEYWORDS AND RESEARCH VARIABLES

4.1. Word cloud Metadata Keyword

The phrase "machine learning" appears most frequently and dominates the word cloud (figure 6) in the metadata produced by keyword analysis in Scopus, demonstrating its significant relevance and wide applicability across numerous academic disciplines (Almorabea et al. 2023). The widespread use of machine learning in domains like artificial intelligence, cybersecurity, anomaly detection, decision systems, and data-driven predictive modeling is reflected in this keyword's prominence (Micro-grid 2023). The steady growth of machine learning-based research is also influenced by the expanding availability of large-scale datasets, improvements in computing power, and integration with cutting-edge technologies like cloud computing and big data analytics (Alhalabi et al., n.d.).

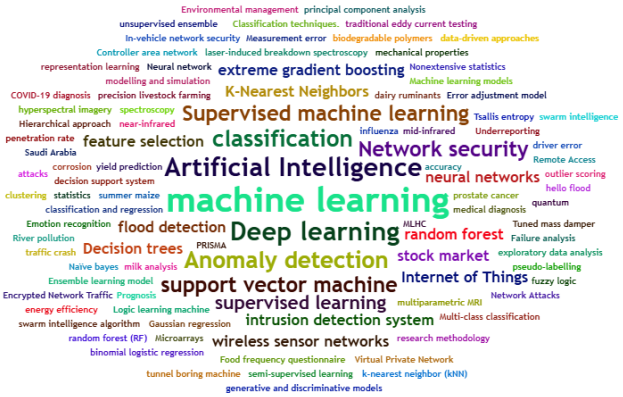

Figure 6. Word cloud Metadata

A number of algorithm-related phrases are frequently found in the extracted keyword structure, indicating that current research focuses on both the notion of machine learning and its model-level implementation(Rafique et al. 2024). Six supervised learning techniques were found to be the most pertinent for Network Flood Detection (NFD) based on the metadata pattern and literature synthesis: KNN, SVM, Random Forest, XGBoost, CNN, and RNN (Al-fuhaidi et al. 2024). These models allow for comparative evaluation across several computational and structural paradigms because they strike a balance between ensemble-based learning, deep learning, and conventional machine learning(Cerdà-alabern, Iuhasz, and Gemmi 2023). Consistent performance in classification tasks, proven adaptability to network traffic data, and aptitude for identifying anomalous patterns in large-scale network systems all support their selection (Farkas 2023).

5. PROPOSED TAXONOMY OF SUPERVISED LEARNING FOR NETWORK FLOOD DETECTION

The fundamental elements of network-based attack detection, such as algorithms, data sources, assessment metrics, and methodological direction, are outlined in the Network Flood Detection (NFD) research framework (C. Networks 2023). This study's taxonomy divides supervised learning techniques into three model groups: deep learning architectures (CNN and RNN), ensemble learning (XGBoost), and classical machine learning (SVM, RF, and KNN), which are frequently employed in cybersecurity classification tasks (Locatelli et al. 2023). To reflect both typical and harmful network behavior, the models are trained and assessed using DDoS-based attack datasets and network traffic datasets (Saeed et al. 2023). To maintain consistency and comparability across experiments, model performance is evaluated using standard machine learning assessment measures, including accuracy, precision, recall, and F1-score (Aljably, Tian, and Al-rodhaan 2020). Figure 7 illustrates the taxonomy for each part in NFD.

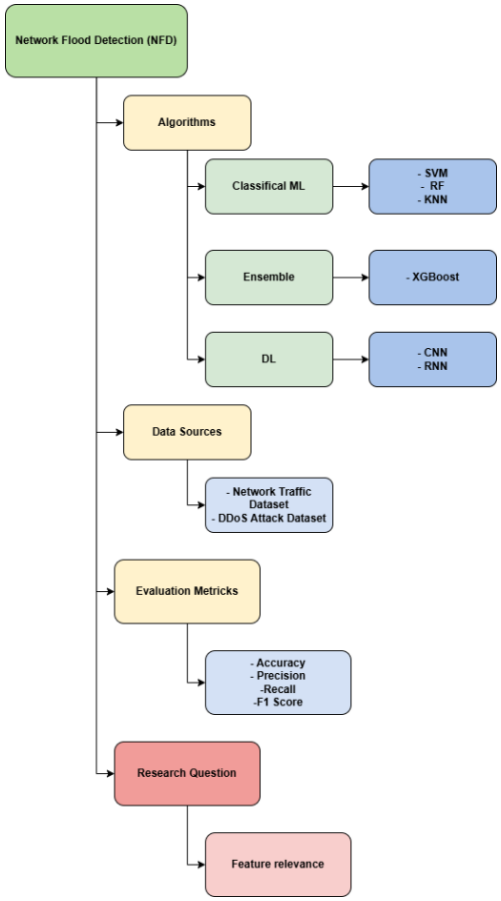

Figure 7. Taxonomy diagram of NFD

Furthermore, this study focuses on finding the most important aspects in enhancing supervised learning-based NFD performance, with the goal of figuring out which traits are most important for accurate and efficient network flood detection (Li 2024). Table 1 shows the detail of each component of NFD taxonomy.

Table 1. Explanation of NFD Taxonomy

Component	Category	Detail
Algorithms	Classical ML	Support Vector Machine (SVM) Random Forest (RF) K-Nearest Neighbor (KNN)
----	Ensemble	XGBoost
----	Deep Learning (DL)	Convolutional Neural Network (CNN) Recurrent Neural Network (RNN)
Data Sources	Network Traffic Dataset DDoS Attack Dataset	Normal and attack network traffic logs Special flood attack datasets (TCP-SYN, UDP Flood, etc.)
Evaluation Metrics	Performance Metrics	Accuracy Precision Recall F1-Score
Research Question	Feature Relevance	Variable number of incoming/outgoing packets, protocol type, bandwidth, IoT traffic patterns, encryption etc

Based on the synthesis results of 40 main articles and 16 supporting articles, this research compiled a taxonomy that describes the Network Flood Detection (NFD) research framework based on supervised learning. This taxonomy aims to provide a systematic classification of algorithms, data sources, evaluation metrics, and the relevance of features used in previous research.

5.1. Algorithms

The algorithms used in Network Flow Detection (NFD) can generally be classified into three main categories: Classical Machine Learning, Ensemble Methods, and Deep Learning (DL). In the Classical Machine Learning category, commonly used algorithms include Support Vector Machine (SVM), Random Forest (RF), and K-Nearest Neighbor (KNN). These classical algorithms dominate research in the field because they provide stable results on labeled datasets and require relatively low computational resources.

The Ensemble Method category is represented by models such as XGBoost, which aim to improve performance through boosting techniques. This approach is particularly effective in handling highly complex data or in situations where maximizing accuracy is a primary objective. The Deep Learning category includes models such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN). These algorithms are suitable for large-scale and complex datasets, especially when analyzing temporal and spatial patterns in network traffic.

5.2. Data Sources

Two main types of data sources are commonly used in NFD research. The first is the Network Traffic Dataset, which contains log data representing both normal and attack traffic on a network. The second is the DDoS Attack Dataset, which specifically represents flooding-based attack scenarios designed to test model performance under high-load conditions.

5.3. Evalution Metrics

Previous studies typically employ standard classification-based metrics to evaluate model effectiveness. The most frequently used metrics are Accuracy, Precision, Recall, and F1-Score, each providing a different perspective on how well a detection model identifies and distinguishes between normal and malicious network activities.

5.4. Research Question

Additionally, this taxonomy links the synthesis results to the research topics that were developed, especially with regard to the function of feature relevance in enhancing detection performance (Hai, Hoang, and Huh 2020). Previous research shows that by capturing crucial traffic parameters including packet frequency, protocol type, bandwidth utilization, and behavioral traffic patterns, good feature selection greatly improves model accuracy, precision, and recall (I. Networks, Alfardus, and Rawat 2024). The taxonomy also shows that algorithm choice, dataset quality, and the appropriateness of extracted features all affect how well supervised learning-based NFD models perform (Katherine et al. 2024). As a result, this study makes a contribution by combining earlier developments and laying the groundwork for future research aimed at creating network flood detection systems that are more precise, dependable, and scalable.

6. RESULTS OF STUDY REVIEW AND ANSWERS TO RESEARCH QUESTIONS

6.1. Study Review Results

The six comparative studies that assess several supervised learning models for Network Flood Detection (NFD), including ensemble techniques, deep learning approaches, and classical algorithms, are summarized in the study review results (table 2). In order to train and assess detection performance, these studies frequently use network traffic parameters including packet count (incoming/outgoing), bandwidth consumption, protocol type, ping fluctuation, and hardware-related network activity as feature inputs. While validation methods like train-test split and k-fold cross-validation are used to guarantee dependable and broadly applicable assessment results, the majority of research quantify performance using accuracy, precision, recall, and F1-score(Chandio et al. 2024). Although fine-tuning is sometimes required to maximize metric balance, ensemble-based models, especially XGBoost and stacking techniques, generally yield strong results.

Table 2. Algorithm and Research Methods Implementation to NFD

Research Method & Algorithm	Accuracy	Precission	F1-Score	Information
KNN	0.93	0.92	0.94	With the second-highest F1-Score and consistent and balanced performance across measures, it is appropriate for NFD environments with distinct and less changeable patterns.
SVM	0.94	0.99	0.99	It exhibits exceptionally accurate classification capabilities and excellent precision to distinguish between regular and flood traffic, making it the algorithm with the best overall performance.
RNN	0.67	0.60	0.71	Its lowest performance in the table suggests that, in the absence of any architectural modifications, this sequence-based technique is not ideal on the utilized NFD dataset.

RF	0.78	0.78	0.78	Provides average and constant performance, being a reasonable baseline but not as competitive as other algorithms in this case.
XGBoost	0.80	0.91	0.87	Demonstrates great precision with little trade-off in accuracy and F1-Score; appropriate for NFDs that need minimizing the false positive rate.
CNN	0.69	0.71	0.77	demonstrates intermediate performance and outperforms RNN; however, for optimal results, architecture adjustment, feature preprocessing, or spatial representation-based datasets are still necessary.

Based on the results the detecting capability of different models varies significantly, according to comparative performance analysis. With exceptional accuracy, precision, and F1-score, SVM performs best. KNN, on the other hand, produces results that are similar and steady despite being sensitive to noise. RNN, on the other hand, performs the worst, suggesting that deeper neural models would need more intricate data representations or architectural modifications to function well in NFD scenarios.While CNN and XGBoost show promise but need more work to produce more balanced results, Random Forest seems to be the most stable model across all evaluation measures, making it a reliable reference baseline. Overall, the results show that deep learning techniques have not yet shown appreciable performance gains without further tuning, whereas conventional supervised learning algorithms especially SVM and KNN remain the most successful for NFD within the assessed dataset(Aytaç, Aydın, and Zaim 2020).

6.2. Answers to Research Questions

RQ : what features are relevant and will greatly influence the performance of NFD?

The review's conclusions demonstrate that feature relevance significantly affects how well Network Flood Detection (NFD) models perform. Features that depict network traffic behavior such as packet rate, flow duration, byte count, payload size, and protocol type have the most impact because they can accurately identify anomalous traffic spikes that are indicative of flooding attempts(Anbar 2020). By identifying departures from typical network patterns, statistical traffic characteristics like entropy, variance, and inter-arrival time also improve detection. For detecting SYN flood and UDP-based attacks, transport-layer characteristics such as TCP flags, connection attempts, and retransmission frequency are crucial.

7. CONCLUSIONS AND RECOMMENDATIONS

This research concludes that algorithm selection, dataset quality, and fitur relevance have a significant impact on the performance of the supervised learning model for Network Flood Detection (NFD). From the several algorithms that are analyzed (KNN, SVM, RF, XGBoost, CNN, and RNN), SVM and KNN provide the best results and the most stable performance under similar traffic conditions, but CNN and RNN are still not ideal without a more complex architecture or representation. Although Random Forest is stable, it does not outperform SVM and KNN.

The following research is aimed at evaluating the model using a larger and more comprehensive dataset based on textual traffic, as well as investigating the hybrid approach between classical and deep learning methods. Fitur optimization, dimension reduction, and real-time or edge computing-based testing are also necessary to improve accuracy, efficiency, and implementation quality in the operational environment.

REFERENCES

Al-fuhaidi, Belal, Zainab Farae, Farouk Al-fahaidy, Gawed Nagi, Abdullatif Ghallab, and Abdu Alameri. 2024. “Anomaly-Based Intrusion Detection System in Wireless Sensor Networks Using Machine Learning Algorithms” 2024. https://doi.org/10.1155/2024/2625922.

Alhalabi, Wadee, Immersive Virtual, Saudi Arabia, Akshat Gaurav, Varsha Arya, Immersive Virtual, Saudi Arabia, et al. n.d. “Machine Learning-Based Distributed Denial of Services (DDoS) Attack Detection in Intelligent Information Systems” 19 (1): 1–17. https://doi.org/10.4018/IJSWIS.327280.

Aljably, Randa, Yuan Tian, and Mznah Al-rodhaan. 2020. “Preserving Privacy in Multimedia Social Networks Using Machine Learning Anomaly Detection” 2020. https://doi.org/10.1155/2020/5874935.

Almorabea, Omar Mohammed, Tariq Jamil Saifullah Khanzada, Muhammad Ahtisham Aslam, Fatheah Ahmad Hendi, and Ahmad Mohammed Almorabea. 2023. “IoT Network-Based Intrusion Detection Framework: A Solution to Process Ping Floods Originating from Embedded Devices.” *IEEE Access* 11 (October): 119118–45. https://doi.org/10.1109/ACCESS.2023.3327061.

AlShaikh, Muath, Yasser Alrajeh, Sultan Alamri, Suhib Melhem, and Ahmed Abu-Khadrah. 2025.

"Supervised Methods of Machine Learning for Email Classification: A Literature Survey." *Systems Science and Control Engineering* 13 (1). https://doi.org/10.1080/21642583.2025.2474450.

Altayef, Ehsan, Fateh Anayi, M. Packianather, Youcef Benmahamed, and Omar Kherif. 2022. "Detection and Classification of Lamination Faults in a 15 KVA Three-Phase Transformer Core Using SVM, KNN and DT Algorithms." *IEEE Access* 10:50925–32. https://doi.org/10.1109/ACCESS.2022.3174359.

Anbar, Mohammed. 2020. "ICMPv6-Based DoS and DDoS Attacks Detection Using Machine Learning Techniques , Open Challenges , and Blockchain Applicability : A Review" 8. https://doi.org/10.1109/ACCESS.2020.3022963.

Aytaç, Tuğba, Muhammed Ali Aydın, and Abdül Halim Zaim. 2020. "Detection DDOS Attacks Using Machine Learning Methods" 20 (2): 159–67. https://doi.org/10.5152/electrica.2020.20049.

Birant, Kokten Ulas. 2023. "Semi-Supervised k-Star (SSS): A Machine Learning Method with a Novel Holo-Training Approach." *Entropy* 25 (1). https://doi.org/10.3390/e25010149.

Cerdà-alabern, Llorenç, Gabriel Iuhasz, and Gabriele Gemmi. 2023. "Anomaly Detection for Fault Detection in Wireless Community Networks Using Machine Learning." *Computer Communications* 202 (September 2022): 191–203. https://doi.org/10.1016/j.comcom.2023.02.019.

Çevik, Nurşah, and Sedat Akleylek. 2024. "SoK of Machine Learning and Deep Learning Based Anomaly Detection Methods for Automatic Dependent Surveillance- Broadcast." *IEEE Access* 12 (March): 35643–62. https://doi.org/10.1109/ACCESS.2024.3369181.

Chandio, Sadullah, Javed Ahmed Laghari, Senior Member, Muhammad Akram Bhayo, Mohsin A L I Koondhar, Yun-su Kim, Senior Member, Besma Bechir Graba, and Ezzeddine Touti. 2024. "Machine Learning-Based Multiclass Anomaly Detection and Classification in Hybrid Active Distribution Networks." *IEEE Access* 12 (September): 120131–41. https://doi.org/10.1109/ACCESS.2024.3445287.

Farkas, Karoly. 2023. "AREP : An Adaptive , Machine Learning-Based Algorithm for Real-Time Anomaly Detection on Network Telemetry Data Pivotal to Understand the Details of Complex Processes And." *Neural Computing and Applications* 35 (8): 6079–94. https://doi.org/10.1007/s00521-022-08000-y.

Fatriansyah, Jaka Fajar, Elvi Kustiyah, Siti Norasmah Surip, Andreas Federico, Agrin Febrian Pradana, Aniek Sri Handayani, Mariatti Jaafar, and Donanta Dhaneswara. 2023. "Fine-Tuning Optimization of Poly Lactic Acid Impact Strength with Variation of Plasticizer Using Simple Supervised Machine Learning Methods." *Express Polymer Letters* 17 (9): 964–73. https://doi.org/10.3144/expresspolymlett.2023.71.

Hai, Tran Hoang, Le Huy Hoang, and Eui-nam Huh. 2020. "N ETWORK A NOMALY D ETECTION B ASED ON L ATE F USION OF S EVERAL M ACHINE" 12 (6): 117–31. https://doi.org/10.5121/ijcnc.2020.12608.

Halder, Rajib Kumar, Mohammed Nasir Uddin, Md Ashraf Uddin, Sunil Aryal, and Ansam Khraisat. 2024. "Enhancing K-Nearest Neighbor Algorithm: A Comprehensive Review and Performance Analysis of Modifications." *Journal of Big Data* 11 (1). https://doi.org/10.1186/s40537-024-00973-y.

Kamamura, Shohei, Yuki Takei, Masato Nishiguchi, Yuhei Hayashi, and Takayuki Fujiwara. 2023. "Network Anomaly Detection Through IP Traffic Analysis With Variable Granularity." *IEEE Access* 11 (October): 129818–28. https://doi.org/10.1109/ACCESS.2023.3334212.

Katherine, Maria, Plazas Olaya, Jaime Alberto, Vergara Tejada, Jose Edinson, and Aedo Cobo. 2024. "Securing Microservices-Based IoT Networks : Real-Time Anomaly Detection Using Machine Learning" 2024. https://doi.org/10.1155/2024/9281529.

Khalid, Waqar, Naveed Ahmed, Muhammad Khalid, Aziz Ud Din, Aurangzeb Khan, and Muhammad Arshad. 2019. "FRID: Flood Attack Mitigation Using Resources Efficient Intrusion Detection Techniques in Delay Tolerant Networks." *IEEE Access* 7:83740–60. https://doi.org/10.1109/ACCESS.2019.2924587.

Kumar, Sudesh, and Sunanda Gupta. 2025. "SDN TCP-SYN Dataset: A Dataset for TCP-SYN Flood DDoS Attack Detection in Software-Defined Networks." *Data in Brief* 59:111314. https://doi.org/10.1016/j.dib.2025.111314.

Li, Rongrong. 2024. "Applied Mathematics and Nonlinear Sciences" 9 (1): 1–16.

Locatelli, Pierluigi, Massimo Perri, Daniel Mauricio, Jimenez Gutierrez, Andrea Lacava, and Francesca Cuomo. 2023. "Device Discovery and Tracing in the Bluetooth Low Energy Domain." *Computer Communications* 202 (September 2022): 42–56. https://doi.org/10.1016/j.comcom.2023.02.008.

Lu, Yutao, Juan Wang, Miao Liu, Kaixuan Zhang, Guan Gui, Tomoaki Ohtsuki, and Fumiyuki Adachi. 2020. "Semi-Supervised Machine Learning Aided Anomaly Detection Method in Cellular Networks." *IEEE Transactions on Vehicular Technology* 69 (8): 8459–67. https://doi.org/10.1109/TVT.2020.2995160.

Micro-grid, Smart. 2023. "Quantum Computing and Machine Learning for Cybersecurity : Distributed Denial of Service (DDoS) Attack Detection On."

Ndichu, Samuel, Sylvester McOyowo, Henry Okoyo, and Cyrus Wekesa. 2023. "Detecting Remote Access Network Attacks Using Supervised Machine Learning Methods." *International Journal of Computer Network and Information Security* 15 (2): 48–61. https://doi.org/10.5815/ijcnis.2023.02.04.

Networks, Communication. 2023. "Retracted : Detection of DDoS Attack within Industrial IoT" 2022. https://doi.org/10.1155/2022/1401683.

Networks, In-vehicle, Asma Alfardus, and Danda B Rawat. 2024. "Machine Learning-Based Anomaly Detection for Securing."

Park, Seunghyun, and Jin Young Choi. 2020. "Hierarchical Anomaly Detection Model for In-Vehicle Networks Using Machine Learning Algorithms." *Sensors (Switzerland)* 20 (14): 1–21. https://doi.org/10.3390/s20143934.

Patel, Pragati, Sivarenjani B, and Ramesh Naidu Annavarapu. 2025. "Application of Supervised Machine Learning Models in Human Emotion Classification Using Tsallis Entropy as a Feature." *Journal of Big Data* 12 (1). https://doi.org/10.1186/s40537-025-01177-8.

Popoola, Anjolaoluwa Ayomide, Jennifer Koren Frediani, Terryl Johnson Hartman, and Kamran Paynabar. 2023. "Mitigating Underreported Error in Food Frequency Questionnaire Data Using a Supervised Machine Learning Method and Error Adjustment Algorithm." *BMC Medical Informatics and Decision Making* 23 (1): 1–11. https://doi.org/10.1186/s12911-023-02262-9.

Puttinaovarat, Supattra, and Paramate Horkaew. 2020. "Flood Forecasting System Based on Integrated Big and Crowdsource Data by Using Machine Learning Techniques." *IEEE Access* 8:5885–5905. https://doi.org/10.1109/ACCESS.2019.2963819.

Radhika, S., K. Anitha, C. Kavitha, Wen Cheng Lai, and S. R. Srividhya. 2023. "Detection of Hello Flood Attacks Using Fuzzy-Based Energy-Efficient Clustering Algorithm for Wireless Sensor Networks." *Electronics (Switzerland)* 12 (1). https://doi.org/10.3390/electronics12010123.

Rafique, Saida Hafsa, Amira Abdallah, Nura Shifa Musa, and Thangavel Murugan. 2024. "Things Network Anomaly Detection — Current Research Trends."

Saeed, Mamoon M, Rashid A Saeed, Maha Abdelhaq, Raed Alsaqour, and Mohammad Kamrul Hasan. 2023. "Anomaly Detection in 6G Networks Using Machine."

Sangodoyin, Abimbola O., Mobayode O. Akinsolu, Prashant Pillai, and Vic Grout. 2021. "Detection and Classification of DDoS Flooding Attacks on Software-Defined Networks: A Case Study for the Application of Machine Learning." *IEEE Access* 9:122495–508. https://doi.org/10.1109/ACCESS.2021.3109490.

Shaik, Riyaaz Uddien, Aiswarya Unni, and Weiping Zeng. 2022. "Quantum Based Pseudo-Labelling for Hyperspectral Imagery: A Simple and Efficient Semi-Supervised Learning Method for Machine Learning Classifiers." *Remote Sensing* 14 (22). https://doi.org/10.3390/rs14225774.

Shajari, Mehdi, Hongxiang Geng, Kaixuan Hu, and Alberto Leon-Garcia. 2022. "Tensor-Based Online Network Anomaly Detection and Diagnosis." *IEEE Access* 10 (August): 85792–817. https://doi.org/10.1109/ACCESS.2022.3197651.

Ullah, Imtiaz, and Qusay H. Mahmoud. 2021. "A Framework for Anomaly Detection in IoT Networks Using Conditional Generative Adversarial Networks." *IEEE Access* 9:165907–31. https://doi.org/10.1109/ACCESS.2021.3132127.

Wang, Fajing, and Xu Feng. 2025. "Flood Change Detection Model Based on an Improved U-Net Network and Multi-Head Attention Mechanism." *Scientific Reports* 15 (1): 1–16.

https://doi.org/10.1038/s41598-025-87851-6.

Wang, Song, Juan Fernando Balarezo, Sithamparanathan Kandeepan, Akram Al-Hourani, Karina Gomez Chavez, and Benjamin Rubinstein. 2021. "Machine Learning in Network Anomaly Detection: A Survey." *IEEE Access* 9:152379–96. https://doi.org/10.1109/ACCESS.2021.3126834.

Wang, Zhimin, Lingli Zhao, Nan Jiang, Weidong Sun, Jie Yang, Lei Shi, Hongtao Shi, and Pingxiang Li. 2025. "DMCF-Net: Dilated Multi-Scale Context Fusion Network for SAR Flood Detection." *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing* PP:1–12. https://doi.org/10.1109/JSTARS.2025.3584282.

Yi, Junkai, and Yongbo Tian. 2024. "Insider Threat Detection Model Enhancement Using Hybrid Algorithms between Unsupervised and Supervised Learning." *Electronics (Switzerland)* 13 (5). https://doi.org/10.3390/electronics13050973.

Zhang, Shichao. 2022. "Challenges in KNN Classification." *IEEE Transactions on Knowledge and Data Engineering* 34 (10): 4663–75. https://doi.org/10.1109/TKDE.2021.3049250.