



INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact Factor: 6.078

(Volume 12, Issue 3 - V12I3-1174)

Available online at: <https://www.ijariit.com>

Hybrid Machine Learning and Deep Learning Approaches for Network Traffic Anomaly Detection: A Literature Review

Abdulhaq Nabizoi

abdulhaqnabizoi@gmail.com

Qassim University, Saudi Arabia

ABSTRACT

Network traffic produces large volumes of data every second, and traditional security tools often struggle to detect new or unknown attacks hidden within this traffic. Anomaly-based intrusion detection systems address this problem by learning normal network behavior and identifying suspicious deviations. This literature review examines recent studies that use machine learning, deep learning, and hybrid machine learning-deep learning approaches for network traffic anomaly detection. The review focuses on feature selection, model complexity, dataset use, evaluation metrics, and the practical challenges that still limit real-world deployment. The reviewed studies show that traditional machine learning models can remain efficient when supported by careful feature selection, while deep learning models are useful for learning more complex spatial and temporal traffic patterns. Hybrid approaches often report stronger performance because they combine the speed and simplicity of machine learning with the representational power of deep learning. However, the literature also shows continuing weaknesses, including reliance on static benchmark datasets, class imbalance, computational cost, limited explainability, and uncertainty about performance in live networks. The review concludes that hybrid approaches are promising, but their future value depends on making them lighter, more explainable, and more reliable outside controlled experimental settings.

Keywords: *Intrusion Detection System, Network Traffic, Anomaly Detection, Machine Learning, Deep Learning, Hybrid Models, Feature Selection.*

1. INTRODUCTION

Modern networks face increasingly complex security threats, especially as more devices, cloud services, web platforms, and smart systems are connected. As the number of connected services grows, the number of possible entry points for attackers also increases. Firewalls and basic antivirus software cannot stop every threat, especially when attackers use techniques that are not yet included in existing security rules. For this reason, administrators rely on intrusion detection systems to monitor traffic, identify suspicious activity, and support early response before an attack causes serious damage.

An intrusion detection system acts as a continuous monitor for network traffic. Older systems rely mainly on signature-based detection. This method works by matching network traffic against predefined rules for known attacks, and an alert is raised when traffic matches one of those rules. Signature-based detection is fast and usually produces fewer false alarms, but it is weak against zero-day attacks because those threats do not yet have known signatures. In modern networks, this weakness is important because attackers may change their behavior, hide malicious traffic inside normal communication, or use new attack patterns that traditional tools cannot recognize.

To detect unknown attacks, researchers and security practitioners have moved toward anomaly-based intrusion detection. Instead of searching only for known malicious patterns, an anomaly-based system learns the normal behavior of a network and flags traffic that deviates too far from that baseline. Machine learning and deep learning have become important in this area because they can process large traffic logs and identify patterns that are difficult for human analysts to notice. These models can support the detection of abnormal flows, unusual packet behavior, rare attack classes, and complex relationships between network features.

Traditional machine learning models are usually lighter and faster, but they depend heavily on the quality of selected features. If the feature set contains irrelevant or repeated information, the model may become slower, less stable, or more likely to produce false alarms. For this reason, feature selection has become an important part of machine learning-based intrusion detection. Recent studies show that methods such as Random Forest, XGBoost, decision-based models, and optimization-based feature selection can improve efficiency and reduce unnecessary computational overhead when applied carefully.

Deep learning models, on the other hand, can learn richer patterns directly from data, but they usually require more training time and stronger computing resources. Models such as Convolutional Neural Networks, Long Short-Term Memory networks, Bidirectional Long Short-Term Memory networks, Autoencoders, and attention-based structures are often used to learn spatial and temporal behavior from network traffic. These models are useful when attack behavior is complex, but they can also be difficult to deploy in real-time environments because of their computational cost and limited explainability.

Because each approach has its own strengths and weaknesses, many recent studies have explored hybrid models that combine machine learning and deep learning in one intrusion detection pipeline. In some studies, machine learning is used for feature selection or final classification, while deep learning is used to learn deeper traffic patterns. In other studies, deep learning extracts features and machine learning classifiers make the final decision. This review compares those studies, discusses their datasets and evaluation metrics, and highlights the research gaps that still prevent many models from being used confidently in real-world networks. The main focus is not only on reported accuracy, but also on class imbalance, false alarms, computational cost, explainability, and the practical difficulty of deploying these models outside controlled benchmark datasets.

2. BACKGROUND OF INTRUSION DETECTION SYSTEMS

Intrusion detection systems are commonly discussed as either host-based intrusion detection systems or network-based intrusion detection systems. A host-based system runs on a single computer or server and observes internal activity, such as changes in important system files, unusual memory behavior, or unauthorized access attempts. A network-based system observes traffic moving between devices in a network. It may inspect packet headers, payload sizes, connection durations, and other traffic characteristics. Most artificial intelligence-based intrusion detection research focuses on network-based systems because modern attacks usually generate large volumes of traffic and often originate outside the protected environment.

From an operational point of view, intrusion detection systems usually depend on either signature-based or anomaly-based detection. Signature-based detection is useful when the attack pattern is already known. Anomaly-based detection is more data-driven. It learns the statistical behavior of normal traffic and then identifies unusual activity. For example, if a server normally receives a limited number of requests per minute, a sudden and unusual spike may indicate suspicious behavior.

Network traffic is represented through features such as source and destination addresses, ports, packet counts, protocol types, and connection duration. When a network contains many devices and services, the feature space becomes large and difficult to analyze manually. Machine learning and deep learning models help by learning mathematical boundaries between normal and abnormal traffic. Once trained, these models can evaluate new traffic and classify it as normal or suspicious.

3. REVIEW METHODOLOGY

This paper follows a focused literature review approach. The review is based on the studies already collected for this topic and cited in the manuscript. The selected works mainly discuss machine learning, deep learning, hybrid intrusion detection models, feature selection, benchmark datasets, and evaluation metrics for network traffic anomaly detection.

The review was organized around four main questions: how traditional machine learning models are used for anomaly detection, how deep learning models improve pattern learning from network traffic, how hybrid machine learning-deep learning approaches combine the strengths of both methods, and what challenges remain before these models can be used reliably in live networks. Based on these questions, the studies were discussed in groups: machine learning and feature selection-based IDS, deep learning-based IDS, hybrid ML-DL IDS, datasets and evaluation metrics, and research gaps and challenges.

Each study was examined according to the method used, the dataset mentioned, the reported performance or main finding, and the limitation discussed in the available material. This organization makes it easier to compare the studies without changing their meaning or adding unsupported details.

To keep the review controlled and honest, no unsupported results were added. Where the available source details were limited, the study was discussed only at the level supported by the provided manuscript. This helps avoid exaggerated claims and keeps the paper aligned with the information available in the reviewed literature.

4. MACHINE LEARNING AND FEATURE SELECTION-BASED IDS

Machine learning models are useful in intrusion detection because they are often lighter than deep neural networks and may be more practical for standard network environments. Decision Trees, Support Vector Machines, Random Forests, XGBoost, AdaBoost, and Logistic Regression are examples of models discussed in the reviewed literature. Their strength is not only classification accuracy, but also practical speed, especially when the number of input features is controlled.

Raw network traffic may include many features, but not all of them are useful. Some features may be irrelevant, repeated, or unstable. If a model receives too many weak features, it may slow down or learn noise instead of meaningful attack behavior. This problem is often linked to overfitting. Feature selection helps by removing unnecessary columns and keeping the most useful indicators for distinguishing normal traffic from attacks.

Balyan et al. [1] showed that reducing the number of features can lower computational overhead while keeping detection performance strong. Emirmahmutoglu and Atay [2] also focused on selecting an optimal subset of features to improve classification speed. Hakke et al. [3] discussed how removing redundant features can reduce false positives and make decisions more stable.

Eljialy et al. [4] applied feature selection methods in software-defined networking and Internet of Things environments. These environments generate large and complex traffic, which can increase false alarms if the model processes unnecessary features. Their work used feature selection with classifiers such as Decision Trees, Random Forests, AdaBoost, XGBoost, and Logistic Regression. Taken together, these studies suggest that traditional machine learning remains valuable when feature selection is handled carefully.

5. DEEP LEARNING-BASED IDS

Deep learning approaches reduce the need for manual feature engineering because neural networks can learn complex representations from data. Models such as Convolutional Neural Networks, Long Short-Term Memory networks, Bidirectional Long Short-Term Memory networks, Autoencoders, Transformers, and attention-based architectures are commonly used in recent intrusion detection studies.

Convolutional Neural Networks are often used to identify spatial patterns in transformed network data, while Long Short-Term Memory and Bidirectional Long Short-Term Memory networks are useful for sequential traffic behavior. Since network packets and flows occur over time, sequence models can capture relationships that simpler classifiers may miss. Fu et al. [5] and Alrayes et al. [6] explored these deep feature learning capabilities and showed that neural networks can identify complex attack patterns in traffic data.

More advanced studies have used attention mechanisms, data balancing methods, Autoencoders, and Transformer-based models. Fu et al. [5] used ADASYN, an improved stacked autoencoder, Convolutional Neural Networks, an attention mechanism, and Bidirectional Long Short-Term Memory to address imbalanced intrusion data. Akkepalli and Sagar [7] proposed a complex model using an Autoencoder-Convolutional Neural Network and a Transformer-Deep Neural Network. Their work also used ADASYN-SMOTE to address uneven data distribution and reported up to 99.98% binary accuracy on CICIDS2017 and NF-BoT-IoT-v2.

A major limitation of deep learning in intrusion detection is its computational cost. Deep neural networks may require specialized hardware, longer training time, and more memory. A complex Transformer-based model may perform well in a laboratory dataset, but it can be difficult to deploy on standard routers or firewalls without increasing latency. This makes real-world deployment a continuing challenge.

6. HYBRID MACHINE LEARNING-DEEP LEARNING-BASED IDS

Hybrid models try to combine the strengths of traditional machine learning and deep learning. In many studies, machine learning is used to clean or select features, and deep learning is used to learn deeper traffic patterns. In other studies, deep learning extracts features and machine learning performs the final classification. This flexibility helps explain why hybrid approaches are increasingly discussed in network traffic anomaly detection research.

Sajid et al. [8] combined XGBoost and Convolutional Neural Networks for feature selection before passing the reduced data to a Long Short-Term Memory model for classification. The study used CICIDS2017, UNSW-NB15, NSL-KDD, and WSN-DS and reported high detection performance with a lower False Acceptance Rate. This structure shows how feature reduction can make deep learning classification more efficient.

Hashmi et al. [9] used a feature-weighted attention-based Bidirectional Long Short-Term Memory model with a Random Forest classifier. The deep learning part processed traffic sequences and highlighted important parts of the data, while the Random Forest made the final classification. Tested on NSL-KDD and UNSW-NB15, the model reported 99.67% and 99.56% binary accuracy, respectively.

Udurume et al. [10] compared a hybrid Convolutional Neural Network-Bidirectional Long Short-Term Memory model with individual machine learning methods such as Logistic Regression, K-Nearest Neighbors, Decision Trees, and Support Vector Machines. The hybrid model achieved 99.89% accuracy on NSL-KDD. Other studies, including Almuhanha and Dardouri [11], Acharya et al. [12], and Kamal and Mashaly [13], also support the value of hybrid designs. However, these models can be difficult to code, tune, and validate in unpredictable enterprise networks.

7. COMPARATIVE ANALYSIS OF REVIEWED STUDIES

The following table summarizes the main studies discussed in this review. It is limited to the information available in the reviewed manuscript and is intended to show the direction, contribution, datasets, and limitations of the selected literature.

8. DATASETS AND EVALUATION METRICS

Intrusion detection research depends heavily on benchmark datasets because testing directly on live enterprise networks may raise privacy and security concerns. The reviewed manuscript discusses several datasets, including NSL-KDD, UNSW-NB15, CICIDS2017, CSE-CIC-IDS2018, WSN-DS, NF-BoT-IoT-v2, and software-defined networking datasets.

NSL-KDD is one of the older and widely used benchmarks. It contains normal traffic and older attack types such as Denial of Service and probing. Although it is useful for baseline comparisons, it does not fully represent modern network threats. UNSW-NB15 includes more recent normal activities and contemporary attack behavior, making it more challenging for classifiers.

CICIDS2017 and CSE-CIC-IDS2018 are popular in recent studies because they include realistic background traffic and modern attack scenarios such as brute force, botnets, Heartbleed, and web attacks. Specialized datasets are also used for specific environments. WSN-DS focuses on wireless sensor networks, NF-BoT-IoT-v2 focuses on Internet of Things botnet behavior, and software-defined networking datasets capture flow-table behavior in programmable networks. The reviewed studies commonly use Accuracy, Precision, Recall, F1-score, False Positive Rate, and False Acceptance Rate. Accuracy measures overall correct predictions, while Precision shows how many flagged attacks were truly attacks. Recall measures how many real attacks were detected. F1-score balances Precision and Recall and is useful when data is imbalanced. False Positive Rate shows how often normal traffic is incorrectly flagged, and False Acceptance Rate shows how often attacks are incorrectly accepted as normal.

9. RESEARCH GAPS AND CHALLENGES

Despite high reported accuracy in many academic studies, anomaly-based intrusion detection still faces several practical challenges. One major challenge is heavy dependence on static benchmark datasets. A model may perform well on CICIDS2017 or NSL-KDD, but real enterprise traffic changes over time. New applications, updates, working hours, and user behavior can shift normal traffic patterns. This creates concept drift and may increase false positives after deployment. Class imbalance is another important issue. In real networks, normal traffic is usually much more common than malicious traffic. If training data does not reflect this imbalance carefully, a model may become too sensitive or may fail to detect rare attacks. High false alarms can also reduce administrators' trust in the intrusion detection system. Computational cost also limits deployment. Some hybrid and attention-based models report very high accuracy, but they may require strong hardware and may not process high-speed traffic in real time. A model that increases latency may be difficult to use in operational network environments. Explainability is also limited. Many machine learning and deep learning models behave like black boxes. When an intrusion detection system flags a connection, administrators need to understand the reason behind the alert. Without explanation, it is hard to decide whether to block traffic, investigate the event, or ignore the alert. Finally, detecting true zero-day attacks remains a difficult challenge. Although anomaly-based systems are designed to detect unknown threats, sophisticated attackers may make malicious traffic look similar to normal behavior. Because most studies evaluate models on known benchmark attacks, the reported accuracy may be more optimistic than the performance expected against truly unseen attacks.

Table-1: Comparative Summary of Reviewed Studies

Study	Approach / Model	Dataset / Environment	Main finding or contribution	Limitation / concern
Balyan et al. [1]	Hybrid IDS using Enhanced Genetic Algorithm, Particle Swarm Optimization, and Improved Random Forest	NSL-KDD	Proposed a hybrid network-based IDS that improves feature selection and classification. Reported 98.979% accuracy for binary classification and 88.149% for multi-class classification.	Mainly tested on benchmark data; real-time enterprise deployment was not clearly demonstrated.
Emirmahmutoglu and Atay [2]	Feature selection-driven ML framework using PSO, FPA, and DE with several ML classifiers	KDDCup99, NSL-KDD, UNSW-NB15, CSE-CIC-IDS2018	Showed that feature selection can improve time efficiency and support high F1-scores across different datasets and classifiers.	Focuses mainly on feature selection and classification performance; live network validation is still limited.
Hakke et al. [3]	Comparative evaluation of several ML classifiers, including SVM, Decision Tree, Random Forest, KNN, AdaBoost, CatBoost, LGBM, LDA, and XGBoost	NSL-KDD, UNSW-NB15, CICIDS2017	Showed that model performance varies strongly across datasets; LGBM performed best on NSL-KDD, while XGBoost performed strongly on UNSW-NB15 and CICIDS2017.	Mainly comparative; does not propose a new hybrid ML-DL model. Very high results on CICIDS2017 require careful interpretation for real-world use.
Eljialy et al. [4]	Multiple feature selection methods with ML classifiers	SDN / IoT environments	Used feature selection with classifiers such as Decision Trees, Random Forests, AdaBoost, XGBoost, and Logistic Regression to reduce false positives and improve detection stability.	Deployment details in real SDN/IoT environments remain limited.
Fu et al. [5]	DLNID model combining ADASYN, improved stacked autoencoder, CNN, attention mechanism, and Bi-LSTM	NSL-KDD	Addressed imbalanced intrusion data and achieved 90.73% accuracy and 89.65% F1-score on KDDTest+.	U2R attacks remained difficult to classify; future work suggested testing the model in an online IDS setting.
Alrayes et al. [6]	Deep Neural Network-based IDS	NSL-KDD	Proposed a DNN-based IDS and reported 91.30% training accuracy and 94.38% validation accuracy.	Focused on NSL-KDD; real-time deployment is suggested but not fully demonstrated.
Akkepalli and Sagar [7]	Autoencoder-CNN and Transformer-DNN with ADASYN-SMOTE	CICIDS2017 and NF-BoT-IoT-v2	Used data balancing and complex deep learning architecture; reported up to 99.98% binary accuracy.	The architecture is complex and may be difficult to deploy in real-time network environments.
Sajid et al. [8]	XGBoost and CNN for feature selection, followed by LSTM classification	CICIDS2017, UNSW-NB15, NSL-KDD, WSN-DS	Hybrid design reported high detection performance and lower False Acceptance Rate.	The model pipeline may require careful tuning across different datasets.
Hashmi et al. [9]	Feature-weighted attention-based BiLSTM with Random Forest classifier	NSL-KDD and UNSW-NB15	Reported 99.67% and 99.56% binary accuracy on NSL-KDD and UNSW-NB15, respectively.	Attention-based hybrid design may be complex for operational deployment.
Udurume et al. [10]	Comparative study of ML models and CNN-BiLSTM deep learning model	NSL-KDD and UNSW-NB15	CNN-BiLSTM achieved 99.89% accuracy on NSL-KDD and 98.95% accuracy on UNSW-NB15.	Results are based on benchmark datasets; live IoT or enterprise deployment needs further validation.
Almuhanna and Dardouri [11]	Hybrid anomaly-based NIDS using ML and DL models, including XGBoost, Random Forest, GNN, LSTM, Autoencoders, SMOTE, and weighted soft-voting ensemble	Large-scale network traffic dataset with over 5.6 million records	Reported near-perfect performance on the primary dataset and used 5-fold cross-validation.	Exact dataset name should be clearly stated if available; real-world deployment is not fully shown.
Acharya et al. [12]	CNN-Bidirectional LSTM hybrid model with sampling strategies	NSL-KDD and UNSW-NB15	Addressed class imbalance and reported strong binary and multiclass anomaly detection performance.	Still benchmark-based; real-world testing and operational validation remain limited.
Kamal and Mashaly [13]	Improved hybrid deep learning IDS using CNN and MLP for binary and multiclass IoT intrusion detection	IoT-23 and NF-BoT-IoT-v2	Reported very high accuracy for binary and multiclass IoT intrusion detection.	Focuses on IoT datasets; generalization to wider enterprise network traffic needs further testing.

10. FUTURE WORK

Future work should move the reviewed ideas toward a practical and manageable intrusion detection prototype that can be tested first on public benchmark datasets and then, if possible, on a controlled lab network. A realistic direction for a master's-level study is to begin with feature selection and class balancing, because the reviewed studies repeatedly show that unnecessary features, imbalanced classes, and false alarms remain major problems in IDS research. A lightweight pipeline could first compare selected machine learning models, such as Random Forest, XGBoost, or related decision-based methods, and then test whether a simple hybrid deep learning component improves detection without creating too much computational cost.

Another useful future direction is to focus less on very high reported accuracy and more on practical measures such as false positive rate, recall for rare attacks, processing time, and model explainability. This would make the work closer to real security operations, where an administrator needs not only an alert, but also a clear reason for that alert. The future prototype should therefore report how many normal flows are incorrectly flagged, how well rare attack classes are detected, and whether the model can run on standard computing resources. Such a direction remains realistic because it can be implemented gradually: first through benchmark datasets such as NSL-KDD, UNSW-NB15, and CICIDS2017, and later through a limited testbed with captured traffic. This path would help connect the literature review with a practical thesis project without making unsupported claims about full real-world deployment.

11. CONCLUSION

This literature review examined machine learning, deep learning, and hybrid approaches for network traffic anomaly detection. Traditional machine learning models remain useful because they are relatively fast and practical, especially when supported by strong feature selection. Deep learning models can learn more complex traffic patterns and identify hidden relationships in large datasets, but they usually require more computational resources. Hybrid approaches are promising because they combine the efficiency of machine learning with the richer representation capability of deep learning.

The reviewed studies show that hybrid models can reach very high accuracy on standard datasets such as NSL-KDD, UNSW-NB15, CICIDS2017, WSN-DS, and NF-BoT-IoT-v2. At the same time, the field still faces serious challenges, including dependence on static datasets, false alarms, class imbalance, computational cost, limited explainability, and uncertain performance in real networks. Future work should therefore focus not only on improving accuracy, but also on building lightweight, explainable, and deployable models that can adapt to changing network behavior.

12. ACKNOWLEDGEMENT

The author acknowledges the academic support received during the preparation of this literature review.

REFERENCES

- [1] Balyan, A. K., Ahuja, S., Lilhore, U. K., Sharma, S. K., Manoharan, P., Algarni, A. D., Elmannai, H., & Raahemifar, K. (2022). A Hybrid Intrusion Detection Model Using EGA-PSO and Improved Random Forest Method. *Sensors*, 22, 5986. <https://doi.org/10.3390/s22165986>
- [2] Emirmahmutoglu, E., & Atay, Y. (2025). A feature selection-driven machine learning framework for anomaly-based intrusion detection systems. *Peer-to-Peer Networking and Applications*, 18, 161. <https://doi.org/10.1007/s12083-025-01947-4>
- [3] Hakke, D. G., Dixit, A. Y., Thorat, S., Malande, G. S., & Panpatte, A. K. (2025). Performance Evaluation of Machine Learning-Based Intrusion Detection Using NSL-KDD, UNSW-NB15 and CICIDS2017 Datasets. *International Journal of Applied Mathematics*, 38(3s), 447-469.
- [4] Eljialy, A., et al. (2024). Multiple Feature Selection Methods Based on Deep Learning for Intrusion Detection in SDN/IoT Networks. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2024.3400012>
- [5] Fu, Y., Du, Y., Cao, Z., Li, Q., & Xiang, W. (2022). A Deep Learning Model for Network Intrusion Detection with Imbalanced Data. *Electronics*, 11, 898. <https://doi.org/10.3390/electronics11060898>
- [6] Alrayes, F. S., Zakariah, M., Amin, S. U., Khan, Z. I., & Alqurni, J. S. (2024). Network Security Enhanced with Deep Neural Network-Based Intrusion Detection System. *Computers, Materials & Continua*. <https://doi.org/10.32604/cmc.2024.051996>
- [7] Akkepalli, S., & Sagar, B. (2025). Autoencoder-CNN and Transformer-DNN with ADASYN-SMOTE for intrusion detection. *Algorithms*, 18(2), 69. <https://doi.org/10.3390/a18020069>
- [8] Sajid, M., et al. (2024). Enhancing Intrusion Detection: A Hybrid Machine and Deep Learning Approach. *Journal of Cloud Computing*, 13, 1-15. <https://doi.org/10.1186/s13677-024-00685-x>
- [9] Hashmi, A., et al. (2024). Feature Weighted Attention-Based DL with Random Forest for anomaly detection. *PLOS ONE*, 19(4), e0302294. <https://doi.org/10.1371/journal.pone.0302294>
- [10] Udurume, M., Shakhov, V., & Koo, I. (2024). Comparative Analysis of Deep Convolutional Neural Network-Bidirectional Long Short-Term Memory and Machine Learning Methods in Intrusion Detection Systems. *Applied Sciences*, 14(16), 6967. <https://doi.org/10.3390/app14166967>
- [11] Almuhanha, R., & Dardouri, S. (2025). A deep learning/machine learning approach for anomaly based network intrusion detection. *Frontiers in Artificial Intelligence*, 8, 1625891. <https://doi.org/10.3389/frai.2025.1625891>
- [12] Acharya, T., Annamalai, A., & Chouikha, M. F. (2024). Enhancing the Network Anomaly Detection using CNN-Bidirectional LSTM Hybrid Model and Sampling Strategies for Imbalanced Network Traffic Data. *Advances in Science, Technology and Engineering Systems Journal*, 9(1), 67-78. <https://dx.doi.org/10.25046/aj090107>
- [13] Kamal, H., & Mashaly, M. (2025). Robust Intrusion Detection System Using an Improved Hybrid Deep Learning Model for Binary and Multi-Class Classification in IoT Networks. *Technologies*, 13(3), 102. <https://doi.org/10.3390/technologies13030102>