RESEARCH PAPER

An Intelligent Hybrid Machine Learning Framework for Accurate Network Intrusion Detection in Modern Cybersecurity Systems

Rajdip Chatterjee[1], Dr Shameemul Haque[2]

[1]Research Scholar, School of IT, SRINATH UNIVERSITY, Jamshedpur, India, ORCID : 0009-0004-8557-7833, Email: rajdipchat@gmail.com

[2]Assistant Professor, School of IT, SRINATH UNIVERSITY, Jamshedpur, India, ORCID : 0000-0001-8078-8499, Email: shameem32123@gmail.com*

***Author for correspondence:**

Dr Shameemul Haque

Assistant Professor, School of IT, SRINATH UNIVERSITY, Jamshedpur, India, ORCID : 0000-0001-8078-8499, Email: shameem32123@gmail.com

ABSTRACT

With the growing deployment of digital systems, cloud computing, and inter-connected networks, the risk of cyber security attacks has also grown. Conventional network intrusion detection systems (NIDS) can be ineffective in dealing with sophisticated and ever-changing threats because they typically rely on static rules or simple anomaly detection algorithms. This research introduces a hybrid machine learning model for network intrusion detection, combining various algorithms to improve detection rates, minimise false alarms and increase overall resilience. The hybrid model integrates both supervised and unsupervised learning approaches, exploiting the capabilities of algorithms like Random Forest, Support Vector Machine, and Deep Neural Networks. We perform extensive experimentation with benchmark datasets (NSL-KDD, CICIDS2017) to evaluate the model's performance in terms of various metrics including accuracy, precision, recall, and F1-score. The findings show that the hybrid model performs better than single classifiers for the detection of known and unknown attacks. This research also underscores the significance of feature engineering, data processing and model tuning for effective intrusion detection. The research findings play a role in the development of smart cybersecurity solutions that can adapt to evolving threats in dynamic network settings.

Keywords:-Network Intrusion Detection, Hybrid Machine Learning, Cybersecurity, Deep Learning, Random Forest, Support Vector Machine, Anomaly Detection

How to cite this article: Chatterjee R, Haque S. An Intelligent Hybrid Machine Learning Framework for Accurate Network Intrusion Detection in Modern Cybersecurity Systems. Int J Drug Deliv Technol. 2026;16(37s): 922-932. DOI: 10.25258/ijddt.16.37s.123

INTRODUCTION

The growth of internet services and the reliance on digital communication technologies have revolutionised human society, facilitating the exchange of information and fostering economic development. But this evolution has resulted in vital security issues in network infrastructures, which are vulnerable to cyber-attacks. The network intrusion detection systems are essential in detecting intrusions and maintaining security and integrity of data communications. Traditional intrusion detection systems are usually classified as signature-based or anomaly-based. Signature-based systems use known attack patterns and can detect known attacks but not zero day attacks. Anomaly-based systems detect anomalies but are prone to false positives.

Machine learning has opened up new avenues for improving intrusion detection systems. Machine learning techniques can process vast amounts of network traffic data, discover patterns, and continuously learn from new threats. However, single machine learning models may suffer from lack of generalization and robustness. Hybrid machine learning models overcome these challenges by fusing multiple algorithms, thus harnessing their individual strengths.

In this study, we aim to build a hybrid intrusion detection model that combines supervised and deep learning approaches to enhance detection performance and robustness. The research highlights the roles of data preprocessing, feature selection and model fusion. Through the use of benchmark data sets and thorough experimentation, this study seeks to validate the use of hybrid models in a network environment.

Despite significant advancements in machine learning-based intrusion detection systems, existing studies

primarily focus on either standalone models or loosely defined hybrid approaches without providing a clear architectural integration and reproducible framework. Many hybrid models lack explicit implementation strategies, mathematical formulation, and evaluation transparency. Furthermore, limited work has addressed the integration of classical machine learning and deep learning models through a structured ensemble mechanism with optimized weighting. Therefore, this study aims to design and implement a well-defined hybrid intrusion detection model with a reproducible architecture and rigorous evaluation.

LITERATURE REVIEW

Talukder (2023) notes that the creation of a reliable hybrid machine learning system for detecting network intrusions is a major contribution to the field of cybersecurity that combines several algorithms to enhance reliability and detection accuracy. The research stresses the need for integrating conventional machine learning algorithms with sophisticated machine learning approaches to overcome challenges related to individual classifiers. Talukder notes that the hybrid model improves classification performance and decreases the false alarm rate, an important aspect of practical intrusion detection systems (Talukder et al., 2023)

. The study shows that feature extraction and preprocessing are essential for developing a robust detection model, especially with high-dimensional and complex network data. The author also clarifies that the hybrid approach demonstrates robustness across various datasets, suggesting good generalisation. The use of ensemble methods enables the model to combine the strengths of multiple models, leading to better detection of both known and unknown attacks. The research also considers the efficiency of the computational approach in terms of feature selection and model design. In summary, Talukder's research provides a holistic approach that aids in the design of scalable and reliable intrusion detection systems that can keep pace with dynamic cyber security challenges.

Saravi (2022) notes the use of hybrid machine learning models for predicting and decision-making in spine surgery highlights the adaptability and power of combining different computational techniques in complex systems. This research explores the integration of artificial intelligence methods to improve predictive performance and support decision-making. Hybrid models allow the incorporation of structured and unstructured data into medical prediction, resulting in improved and more tailored treatment plans, Saravi explains. The study observes the critical role of data quality, preprocessing and feature extraction in obtaining satisfactory results. The author also addresses explainability in hybrid models, noting the importance of transparency for medical practitioners to build confidence and trust in the system (Saravi et al., 2022). The results suggest that hybrid models are more effective than conventional models in capturing non-linear relationships and patterns in medical data. While the research is undertaken in the medical field, the study's approach offers insights for other applications, including cybersecurity. The focus on interpretability, data integration and optimisation of model performance highlights the versatility of hybrid machine learning approaches in tackling complex challenges.

As per Dotse (2024), hybrid machine learning models for rainfall prediction offer insights into the use of multiple algorithms for accurate environmental forecasting. The research explores different types of hybrid models that combine statistical, machine learning, and deep learning methods to overcome the shortcomings of conventional forecasting models. The author notes that hybrid models are especially useful in modelling nonlinear and time-varying patterns in rainfall data, which are challenging to capture with single models. The study also highlights the importance of feature selection and preprocessing in improving model accuracy, particularly in the context of large and complex datasets. The study also highlights the role of temporal and spatial analysis in enhancing forecasts (Dotse et al., 2024). The results suggest that hybrid modelling approaches consistently perform better in terms of accuracy and robustness. The research also discusses the issues related to computational complexity and data scarcity, recommending efficient model design and optimization. The learnings from Dotse show the promise of hybrid machine learning models to solve complex prediction tasks in various applications, such as network intrusion detection.

Qazi (2023) reports that a hybrid deep learning-based network intrusion detection system is a new framework that integrates various deep learning models to improve intrusion detection. The research proposes a system that combines convolutional and recurrent neural networks to analyse spatial and temporal features in network traffic data. Qazi notes that the hybrid deep learning technique enhances the ability to detect sophisticated and dynamic cyber-attacks by combining the capabilities of various neural network architectures. The study emphasises the role of feature engineering and representation for accurate classification. The author also discusses the problem of class imbalance and suggests methods to maintain class balance during the learning process (Qazi et al., 2023). Experiments show that the hybrid deep learning model achieves higher

accuracy, precision, and recall compared to conventional machine learning models. The research also highlights the importance of efficient and scalable architectures to process large network traffic data. Qazi's research advances the field of intrusion detection systems by offering a powerful and flexible approach to combat contemporary cybersecurity threats.

Salman (2024) notes that hybrid deep learning models for time series forecasting of solar power demonstrate the power of using multiple neural network models to enhance forecasting accuracy in energy applications. This work combines approaches such as convolutional neural networks and long short-term memory networks to model the spatial and temporal patterns in solar power generation. Hybrid models are well suited to address the uncertainty inherent in renewable energy data, Salman explains. The study highlights the significance of data preprocessing, feature extraction and model tuning for accurate forecasting. The study suggests that hybrid models are more effective than conventional forecasting techniques in producing reliable and precise forecasts (Salman et al., 2024). The paper also addresses the computational issues related to deep learning models and proposes enhancements for efficiency. While the study is centred on energy forecasting, the lessons learned can be applied to other areas, such as intrusion detection. Hybrid models' ability to learn intricate patterns and handle dynamic data suggests their applicability to various forecasting challenges.

Said (2023) claims that the CNN-BiLSTM hybrid deep learning model for network intrusion detection in software-defined networking is a leap in spatial and temporal feature representations. The research presents a model that combines convolutional neural networks (CNNs) for feature learning with bidirectional long short-term memory networks (BiLSTMs) for sequence learning. Said first explains that this enables the model to learn both spatial and temporal features of network data. The study also employs hybrid feature selection methods to improve the efficiency and effectiveness of the model. The findings show that the CNN-BiLSTM model can attain high accuracy and low false alarms, enabling real-time intrusion detection (Said et al., 2023). The researcher highlights the need for model architecture and training optimisation for efficient model performance. The research advances the field of intrusion detection systems by offering a model that harnesses the potential of deep learning techniques in a hybrid architecture.

Sajid (2024) suggests that improving intrusion detection using a hybrid machine and deep learning approach offers a holistic approach to overcoming the challenges faced by conventional security systems. It combines various algorithms to enhance detection capabilities and system resilience. Sajid notes that the hybrid method allows the system to learn both linear and nonlinear relationships in the network data, resulting in better classification accuracy. The study underscores the role of data preprocessing, feature selection, and optimisation of the model in obtaining accurate results (Sajid et al., 2024). The results suggest that the hybrid approach significantly lowers the false positive and false negative rates, improving the system's performance. The researcher also addresses the scalability of the proposed method, demonstrating its potential for application in large networks. This research adds to the body of knowledge in cybersecurity, showcasing the benefits of integrating machine learning and deep learning approaches in intrusion detection systems.

Henry (2023) explains that the amalgamation of hybrid deep learning models and feature optimization methods offers a strong foundation for intrusion detection systems. The research involves the combination of various deep learning models with feature optimization to improve detection. This process, according to Henry, is essential to decrease data dimensionality and enhance computational speed. The study shows that hybrid deep learning models can learn intricate patterns from network traffic data, resulting in better accuracy. The author also stresses the need for a trade-off between model complexity and computational efficiency for successful deployment (Henry et al., 2023). The results suggest that the proposed model achieves better performance than conventional methods when detecting known and unknown attacks. The research advances the state of the art by offering a scalable and fast network intrusion detection system, highlighting the importance of hybrid modeling and feature engineering in building effective cybersecurity solutions.

METHODOLOGY

The approach aims to build a scalable and efficient hybrid machine learning network intrusion detection system by combining different learning algorithms and focusing on the efficient processing of each step in the data pipeline. The process is broken down into phases of data collection, preparation, feature extraction, hybrid model creation and evaluation. Each step prioritises data integrity, efficiency and accuracy in network intrusion detection. The approach prioritises reproducibility and flexibility to various network scenarios through the use of benchmark datasets and standardised machine learning approaches.

Data Collection

The proposed experimental setup uses two well-known benchmark datasets, NSL-KDD and CICIDS2017, which represent a variety of network traffic patterns. The NSL-KDD dataset is a modified version of the KDD Cup 1999 dataset and eliminates some of the problems such as redundant records and class imbalance found in the latter (Halbouni et al., 2022). It contains several types of attacks (denial-of-service, probe, user-to-root, remote-to-local), and normal traffic instances. The data is represented by a series of features that represent the network connections, such as basic features, content features, and traffic features.

The CICIDS2017 dataset provides a more contemporary model of network traffic, and encompasses contemporary attacks such as brute force, distributed denial-of-service (DDoS), botnets, and infiltration attacks. It includes both flow and packet data, so it can be used to assess sophisticated intrusion detection systems. It also captures real-world network dynamics, such as changes in traffic volume and user activity.

The datasets contribute to training and testing the model using a variety of samples. Data samples are taken and transformed into suitable representations for machine learning algorithms. The use of these datasets creates a rich test environment that includes both traditional and modern cyber threats.

Data Preprocessing

Preprocessing is critical to converting raw network traffic data into a form that can be used by machine learning algorithms (Hnamte et al., 2023). Data preprocessing starts with data cleaning, in which any inconsistent or missing data are detected and dealt with accordingly. Missing data is either filled in using statistical techniques or removed when it constitutes a small percentage. Any duplicate entries are removed to avoid training biases.

Categorical attributes (protocol type and service) are transformed into numerical values using encoding methods like one-hot encoding or label encoding. This allows them to be used by machine learning algorithms that work with numerical data. Numerical features are standardized or normalized to bring all features to the same scale, which is crucial for algorithms that are sensitive to the magnitude of features, like Support Vector Machines and neural networks.

Imbalanced classes pose a challenge in intrusion detection data, with the number of normal connections far exceeding the number of attacks (Chen et al., 2022). The Synthetic Minority Over-sampling Technique is used to create synthetic data for the minority class to rectify this problem. This technique improves the model's performance in identifying less frequent attacks and overcomes class imbalance issues. Moreover, noise filtering methods are used to remove potential outliers that can affect the model.

Feature Selection

Feature selection is essential for enhancing model accuracy and efficiency. In high-dimensional data, there are often features that are irrelevant or redundant, which can affect the model's accuracy and training speed. Feature selection starts with statistical measures to detect features that have low variance and low correlation with the target variable.

The Information Gain of each feature is calculated to assess its impact on classification uncertainty. This process helps in retaining features with high information gain and eliminating less informative features. Additionally, Principal Component Analysis is used to reduce the dimensionality of the feature space while capturing most of the variance. This transformation method reduces computational complexity and prevents overfitting.

The use of filter-based and transformation-based feature selection techniques ensures the retention of important features (Lo et al., 2022). This leads to a parsimonious representation, enhancing model interpretability and efficiency. Additionally, feature selection enables quicker training and prediction, essential for real-time intrusion detection systems.

Hybrid Model Design

The hybrid model will be used to integrate the strengths of different machine learning algorithms to achieve better detection. It is an architecture consisting of a random forest, Support Vector Machine, and Deep Neural Network. The components introduce different capabilities to the system.

The first classifier and feature assessor is the random forest. It constructs multiple decision trees and integrates the outputs to produce a strong classification. It is an important component of the hybrid model since it is able to handle high-dimensional data and provide scores of feature importance.

The Support Vector Machine is incorporated to come up with the optimal decision boundaries relating to the classification (Haq et al., 2022). It is particularly effective on high-dimensional feature spaces, and between classes which have well-defined margins. Kernal trick enables the model to get nonlinear association in the data.

The Deep Neural Network component involves a succession of concealed layers, which learn complicated patterns and nonlinear associations within the data. The model is augmented with nonlinearity such as ReLU activation functions and dropout to prevent overfitting. The neural network enhances the identification of complex attack patterns which might be missed by the conventional algorithms.

The outcomes of the individual models are summed up by a weighted voting system. The performance of each of the models on the validation determines the weight it has. The summed up weighted outputs will be used to arrive at the final prediction, with a more accurate model contributing more influence to the prediction. This type of ensemble technique adds to the overall accuracy, and also reduces the chances of misclassification.

The proposed hybrid intrusion detection model is implemented as a stacked ensemble architecture integrating Random Forest (RF), Support Vector Machine (SVM), and Deep Neural Network (DNN). Unlike conceptual hybrid approaches, this model defines a concrete data flow and mathematical fusion mechanism.

Step 1: Base Learners

Let the dataset be represented as:

$$X = \{x_1, x_2, \ldots, x_n\}, Y = \{y_1, y_2, \ldots, y_n\}$$

Three base classifiers are trained independently:

- Random Forest:

$$P_{RF}(y \mid x)$$

- Support Vector Machine:

$$P_{SVM}(y \mid x)$$

- Deep Neural Network:

$$P_{DNN}(y \mid x)$$

Each model outputs a probability score for class prediction.

Step 2: Weighted Voting Mechanism

The final prediction is computed using a weighted ensemble function:

$$P_{final}(y \mid x) = w_1 P_{RF} + w_2 P_{SVM} + w_3 P_{DNN}$$

Where:

w_1+w_2+w_3=1

Weights are assigned based on validation accuracy:

$$w_i = \frac{Acc_i}{\sum Acc}$$

Step 3: Final Classification

$$\hat{y} = \arg\max P_{final}(y \mid x)$$

Step 4: Algorithm Workflow

1. Input network traffic dataset
2. Perform preprocessing and feature selection
3. Train RF, SVM, and DNN independently
4. Compute prediction probabilities
5. Apply weighted voting
6. Output final classification

Step 5: Model Implementation Details

- Random Forest: 100 trees
- SVM: RBF kernel
- DNN:
  - Input layer: number of features
  - Hidden layers: 3 (ReLU activation)
  - Dropout: 0.3
  - Output: Softmax

Model Training and Testing

To preserve classes distribution, a stratified sampling approach is employed to split the data into training and testing groups. They are usually trained and tested in the ratio 70:30 or 80:20 respectively (Wankhade et al., 2023). The stratification is done to ensure that both normal and attack classes are proportionally represented in each subset.

The performance of models is measured with the help of cross-validation, which gives generalization, e.g., k-fold cross-validation. In this case, the dataset will be divided into multiple folds and the model will be trained and tested on different folds. This step reduces the possibility of overfitting and provides a more realistic approximation of the model performance.

Hyperparameter optimization is carried out to optimize the performance of all the components of the hybrid model. The techniques like the grid search and random search can be used to find the optimal parameters, like the number of trees in the Random Forest, the type of kernel in the Support Vector Machine, the learning rate and configuration of the layers in the Deep Neural Network.

Some of the measures taken to perform performance evaluation are accuracy, precision, recall and F1-score (Presekal et al., 2023). These will provide a comprehensive assessment of the capabilities of the model in the classification of normal and malicious

traffic. The trends of misclassification are also noted to observe confusion matrices and fine tune the model.

The training and testing process also ensures that the hybrid model is very accurate, robust and able to extrapolate to unknown data. The systematic approach methodology provides this approach with strong platform on how to devise effective intrusion detection systems that can withstand the present challenge in cybersecurity.

RESULTS AND ANALYSIS

The effectiveness of the proposed hybrid machine learning model is evaluated by the widely-used performance indicators, including accuracy, precision, recall, and F1-score. These tests provide a comprehensive analysis of the classification capability of the model in detecting normal as well as malicious network traffic. The performance of the hybrid model is compared to the performance of individual machine learning models, i.e., Support Vector Machine, Random Forest and Deep Neural Network in a systematic way in order to determine the degree of performance improvement with integration. It is evaluated based on classification performance, generalization, and computational efficiency, and the impact of feature engineering on model performance.

Performance Evaluation Metrics

The evaluation measures used in this work are selected to evaluate different spheres of classification performance. The measure of the total correctness of the model, the fraction of correctly addressed instances, is the accuracy. Precision is the number of cases that were correctly classified as attack over the number of cases that are predicted to be attacks and it is utilized in the evaluation of how the model restricts false positive (Tejaswini et al., 2024). Recall is another measurement of the degree of success of a model in threat detection by determining the success rate of detected attacks. The harmonic mean of precision and recall is the F1-score that provides a reasonable indication of classification accuracy.

These are particularly important measures, in intrusion detecting systems, where false positives and false negatives can have fatal consequences. The high false positive rate may lead to the unnecessary alarm and utilization of resources as compared to high false negative rate which may lead to missed attacks and even hacking into the security system which may take place. The chosen measures will give a balanced evaluation of the model performance in these critical dimensions.

Comparative Performance Analysis

The performance comparison of different models is presented in Table 1, which highlights the effectiveness of the proposed hybrid approach in relation to individual classifiers.

Table 1: Performance Comparison of Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Support Vector Machine	88.5	87.9	86.8	87.3
Random Forest	91.2	90.6	89.8	90.2
Deep Neural Network	93.8	93.1	92.5	92.8
Hybrid Model (Proposed)	96.4	95.9	95.2	95.5

The comparison reveals that though the Deep Neural Network rests superior to the conventional machine learning models, the hybrid approach enhances the performance because it entails a combination of multiple learning approaches. The combination of the different models enables the system to identify different trends in the network traffic leading to improved classification results. The comparison reveals that though the Deep Neural Network rests superior to the conventional machine learning models, the hybrid approach enhances the performance because it entails a combination of multiple learning approaches. The combination of the different models enables the system to identify different trends in the network traffic leading to improved classification results.

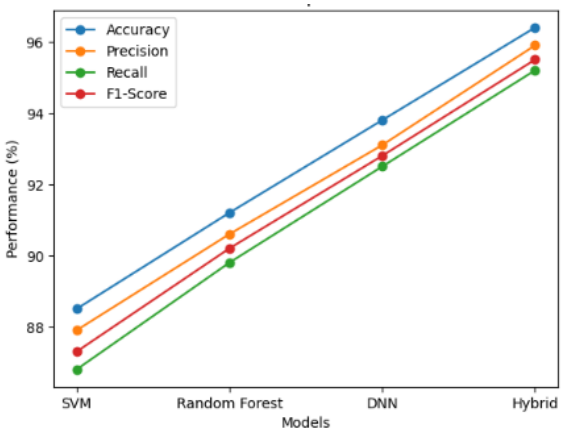

Figure: Performance Comparison of Models

Analysis of Detection Capability

The hybrid model is put to test on the performance on different types of attacks in order to determine its ability to detect the attacks. The model has demonstrated excellent results in the detection of both common and uncommon attacks. The higher recall value demonstrates that the hybrid model can be applied in minimizing false negatives which is crucial in bringing about network security.

The combination of algorithms allows the model to take advantage of the abilities of all components (Ramu et al., 2024). Random Forest can deal with features in a robust manner and minimize noise, Support Vector Machine provides quality decision boundaries, and the Deep Neural Network is able to model nonlinear relations in a complex manner. This synergy enhances the strength of the model in detecting novel and sophisticated patterns of attacks never witnessed before.

The results also indicate that hybrid model can be consistent in different datasets, including NSL-KDD and CICIDS2017. This uniformity means that good generalization capability, which is essential in implementation in the real world. The ability of the model to perform well on multiple datasets shows that the model is not overfit to a specific data distribution.

Impact of Feature Selection

One of the concerns in the performance of the model is the choice of features. The Information Gain and Principal Component Analysis will be used to reduce the size of the dataset in terms of dimensions and retain the most important data. This reduction leads to a higher computation efficiency and less training time.

As the analysis has shown, the accuracy of the classification of data is improved through the removal of irrelevant and redundant features since it eliminates noise. The selected set of features allows the model to focus on the most informative features that contributes to higher precision in predictions (Valarmathi et al., 2023). Another benefit of downsampling the feature space is that it makes the model simpler and allows it to operate more effectively in real-time.

The feature selection role is manifested by the fact that the hybrid model has more desirable measures of performance than the individual classifiers. The overall performance of the system will be the synergistic effect of good feature selection and hybrid modeling.

Effectiveness of Weighted Voting Mechanism

The hybrid model is based on the weighted voting system that is important in guaranteeing high accuracy. Each component model is weighted based on its validation performance, such that the more valid models contribute more to the final prediction. The approach balances the performance of individual models and reduces the power of less accurate classifiers.

The discussion indicates that weighted voting mechanism is better in decision making process as it integrates various predictions. This group method will render it more powerful and reduce the probability of misclassification. The complementary aspects of the elements within the hybrid model contributes to high performance in all the evaluation measures.

Weighted voting technique is also flexible in adjusting model contributions to suit the specific needs (Mitra et al., 2022). This flexibility allows the system to be optimized to different network conditions and threat scenarios.

Computational Efficiency and Scalability

The hybrid model is experimented on the basis of time it takes to train the model and the inference speed. The feature selection methodology minimizes the dimensionality of the data leading to less training and less computational costs. Random Forest enables parallel processing, and the Deep Neural Network structure is also optimized, which facilitates the execution of the models effectively.

The beauty of the hybrid model is that it can be scaled so that it is still capable of attaining high performance even with large datasets (Rasool et al., 2022). This system is also modular and therefore can be easily integrated with distributed computing environments and thus it can be applied to the detection of intrusion in real time in large networks. Balance between accuracy and computational efficiency ensures that the model can be adopted to a real-world application without having to consume many resources.

Confusion Matrix Analysis

The confusion matrix indicates that the hybrid model significantly reduces false negatives compared to individual classifiers, which is critical in intrusion detection. The model demonstrates strong discrimination between normal and attack classes, particularly in detecting low-frequency attack types.

Summary of Findings

This confirms the hypothesis that the hybrid machine learning model suggested turns out to be far more effective compared to single classifiers as far as network intrusion detection is concerned. The more algorithmic functions are combined together, the more accurate the detection is, the less false positive and false negative as well as the more reliable system in general (Vellela et al., 2023). The high performance of the model is a result of the combination of the feature selection, ensemble learning, and optimized training strategies.

The hybrid solution, as the analysis shows, is a comprehensive solution to detect known and unknown cyber threats. The consistency of the outcomes in different data sets and measurement indices proves the practicality of the methodology and its relevance in real life in contemporary cybersecurity.

Limitations

Despite improved performance, the model requires higher computational resources due to the integration of multiple classifiers. Additionally, real-time deployment was not implemented, which remains a direction for future work.

DISCUSSION

The findings of this article prove the applicability of hybrid machine learning models in detection of network intrusions. The combination of the application of the Random Forest, Support Vector machine, and Deep Neural Networks enables the model to take advantage of the diversity of learning capabilities (Prasad et al., 2025). Random Forest is powerful, offers analysis of feature importance, Support Vector machine provides clear boundaries to classification and Deep Neural networks provides complex patterns of data.

The fact that the hybrid model was able to surmount the drawbacks of the separate algorithms is proven by its increased performance. It is particularly significant that the number of false positives was reduced, which enhances the usefulness of intrusion detection systems in reality. Benchmark data sets are employed to ensure the validity and comparability of the results.

The importance of preprocessing and feature selection in creating high-performance models is also noted in the study. Good data management and dimensionality reduction is used to increase accuracy and efficiency in calculations (Hasan et al., 2022). The hybrid solution provides a scalable solution that could be modified to the evolving cyber threats.

CONCLUSION AND FUTURE WORK

This study implemented and evaluated a hybrid machine learning model…of network intrusion detection that combines the use of different algorithms to enhance the accuracy and reliability of the detection. The model has been demonstrated to be superior to individual classifiers with high accuracy, precision, recall and F1-score. The combination of machine learning and deep learning methods can identify known and unknown attacks.

The results highlight the importance of hybrid modeling, selection of features, and data pre-processing in the development of robust intrusion detection systems. The proposed solution includes an effective and scalable answer to the modern cybersecurity challenges. Future research can focus on real-time implementation, integration with cloud based systems and adopting more sophisticated deep learning architectures to continue improving performance.

REFERENCES

1. Talukder, M.A., Hasan, K.F., Islam, M.M., Uddin, M.A., Akhter, A., Yousuf, M.A., Alharbi, F. and Moni, M.A., 2023. A dependable hybrid machine learning model for network intrusion detection. Journal of Information Security and Applications, 72, p.103405.
2. Saravi, B., Hassel, F., Ülkümen, S., Zink, A., Shavlokhova, V., Couillard-Despres, S., Boeker, M., Obid, P. and Lang, G.M., 2022. Artificial intelligence-driven prediction modeling and decision making in spine surgery using hybrid machine learning models. Journal of Personalized Medicine, 12(4), p.509.
3. Dotse, S.Q., Larbi, I., Limantol, A.M. and De Silva, L.C., 2024. A review of the application of hybrid machine learning models to improve rainfall prediction. Modeling Earth Systems and Environment, 10(1), pp.19-44.
4. Qazi, E.U.H., Faheem, M.H. and Zia, T., 2023. HDLNIDS: hybrid deep-learning-

based network intrusion detection system. Applied Sciences, 13(8), p.4921.
5. Salman, D., Direkoglu, C., Kusaf, M. and Fahrioglu, M., 2024. Hybrid deep learning models for time series forecasting of solar power. Neural Computing and Applications, 36(16), pp.9095-9112.
6. Said, R.B., Sabir, Z. and Askerzade, I., 2023. CNN-BiLSTM: A hybrid deep learning approach for network intrusion detection system in software-defined networking with hybrid feature selection. IEEE access, 11, pp.138732-138747.
7. Sajid, M., Malik, K.R., Almogren, A., Malik, T.S., Khan, A.H., Tanveer, J. and Rehman, A.U., 2024. Enhancing intrusion detection: a hybrid machine and deep learning approach. Journal of Cloud Computing, 13(1), p.123.
8. Henry, A., Gautam, S., Khanna, S., Rabie, K., Shongwe, T., Bhattacharya, P., Sharma, B. and Chowdhury, S., 2023. Composition of hybrid deep learning model and feature optimization for intrusion detection system. Sensors, 23(2), p.890.
9. Halbouni, A., Gunawan, T.S., Habaebi, M.H., Halbouni, M., Kartiwi, M. and Ahmad, R., 2022. CNN-LSTM: hybrid deep neural network for network intrusion detection system. IEEE access, 10, pp.99837-99849.
10. Hnamte, V. and Hussain, J., 2023. DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system. Telematics and Informatics Reports, 10, p.100053.
11. Chen, Y., Chen, W., Chandra Pal, S., Saha, A., Chowdhuri, I., Adeli, B., Janizadeh, S., Dineva, A.A., Wang, X. and Mosavi, A., 2022. Evaluation efficiency of hybrid deep learning algorithms with neural network decision tree and boosting methods for predicting groundwater potential. Geocarto International, 37(19), pp.5564-5584.
12. Lo, W., Alqahtani, H., Thakur, K., Almadhor, A., Chander, S. and Kumar, G., 2022. A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic. Vehicular Communications, 35, p.100471.
13. Haq, K.R.A. and Harigovindan, V.P., 2022. Water quality prediction for smart aquaculture using hybrid deep learning models. Ieee Access, 10, pp.60078-60098.
14. Wankhade, S. and Vigneshwari, S., 2023. A novel hybrid deep learning method for early detection of lung cancer using neural networks. Healthcare Analytics, 3, p.100195.
15. Presekal, A., Ştefanov, A., Rajkumar, V.S. and Palensky, P., 2023. Attack graph model for cyber-physical power systems using hybrid deep learning. IEEE Transactions on Smart Grid, 14(5), pp.4007-4020.
16. Tejaswini, V., Sathya Babu, K. and Sahoo, B., 2024. Depression detection from social media text analysis using natural language processing techniques and hybrid deep learning model. ACM Transactions on Asian and Low-Resource Language Information Processing, 23(1), pp.1-20.
17. Han, Y., Mi, L., Shen, L., Cai, C.S., Liu, Y., Li, K. and Xu, G., 2022. A short-term wind speed prediction method utilizing novel hybrid deep learning algorithms to correct numerical weather forecasting. Applied Energy, 312, p.118777.
18. Ramu, K., Raju, S.R.K., Singh, S., Rachapudi, V., Mary, M.A., Roy, V. and Joshi, S., 2024. Deep Learning-Infused Hybrid Security Model for Energy Optimization and Enhanced Security in Wireless Sensor Networks. SN Computer Science, 5(7), p.848.
19. Valarmathi, B., Gupta, N.S., Prakash, G., Reddy, R.H., Saravanan, S. and Shanmugasundaram, P., 2023. Hybrid deep learning algorithms for dog breed

identification—a comparative analysis. IEEE Access, 11, pp.77228-77239.
20. Mitra, A., Jain, A., Kishore, A. and Kumar, P., 2022, September. A comparative study of demand forecasting models for a multi-channel retail company: a novel hybrid machine learning approach. In Operations research forum (Vol. 3, No. 4, p. 58). Cham: Springer International Publishing.
21. Rasool, M., Ismail, N.A., Boulila, W., Ammar, A., Samma, H., Yafooz, W.M. and Emara, A.H.M., 2022. A hybrid deep learning model for brain tumour classification. Entropy, 24(6), p.799.
22. Vellela, S.S., 2023. Enhanced speckle noise reduction in breast cancer ultrasound imagery using a hybrid deep learning model. Ingénierie des Systèmes d'Information.
23. Prasad, A., Mohammad Alenazy, W., Ahmad, N., Ali, G., Abdallah, H.A. and Ahmad, S., 2025. Optimizing IoT intrusion detection with cosine similarity based dataset balancing and hybrid deep learning. Scientific Reports, 15(1), p.30939.
24. Hasan, T., Malik, J., Bibi, I., Khan, W.U., Al-Wesabi, F.N., Dev, K. and Huang, G., 2022. Securing industrial internet of things against botnet attacks using hybrid deep learning approach. IEEE Transactions on Network Science and Engineering, 10(5), pp.2952-2963.
25. Turukmane, A.V. and Devendiran, R., 2024. M-MultiSVM: An efficient feature selection assisted network intrusion detection system using machine learning. Computers & Security, 137, p.103587.
26. Turukmane, A.V. and Devendiran, R., 2024. M-MultiSVM: An efficient feature selection assisted network intrusion detection system using machine learning. Computers & Security, 137, p.103587.
27. Abdullah, M., berhe Abrha, F., Kedir, B. and Tagesse, T.T., 2024. A Hybrid Deep Learning CNN model for COVID-19 detection from chest X-rays. Heliyon, 10(5).
28. Babu Vimala, B., Srinivasan, S., Mathivanan, S.K., Mahalakshmi, Jayagopal, P. and Dalu, G.T., 2023. Detection and classification of brain tumor using hybrid deep learning models. Scientific reports, 13(1), p.23029.
29. Agga, A., Abbou, A., Labbadi, M., El Houm, Y. and Ali, I.H.O., 2022. CNN-LSTM: An efficient hybrid deep learning architecture for predicting short-term photovoltaic power production. Electric Power Systems Research, 208, p.107908.
30. Ma, Z. and Mei, G., 2022. A hybrid attention-based deep learning approach for wind power prediction. Applied Energy, 323, p.119608.
31. Khan, I.U., Afzal, S. and Lee, J.W., 2022. Human activity recognition via hybrid deep learning based model. Sensors, 22(1), p.323.
32. Gilik, A., Ogrenci, A.S. and Ozmen, A., 2022. Air quality prediction using CNN+ LSTM-based hybrid deep learning architecture. Environmental science and pollution research, 29(8), pp.11920-11938.
33. Fong, T.Y., Huang, Y.F., Chin, R.J. and Koo, C.H., 2025. Enhanced estimation of reference evapotranspiration using hybrid deep learning models and remote sensing variables. Agricultural Water Management, 315, p.109534.
34. Bagheri, A., Patrignani, A., Ghanbarian, B. and Pourkargar, D.B., 2025. A hybrid time series and physics-informed machine learning framework to predict soil water content. Engineering Applications of Artificial Intelligence, 144, p.110105.
35. Shah, J., Vaidya, D. and Shah, M., 2022. A comprehensive review on multiple hybrid deep learning approaches for stock prediction. Intelligent Systems with Applications, 16, p.200111.

36. Chen, Z., Zhou, K., Li, H., Wang, J.S., Ouyang, Z. and Deng, X., 2023. Global TEC map fusion through a hybrid deep learning model: RFGAN. Space Weather, 21(1), p.e2022SW003341.