Technoscience Journal for Community Development in Africa 5:1 (2026) 1–9
ISSN 2659-0573

Research Article

A stack ensemble approach to intrusion detection based on decision tree and bayesian network algorithms

Oluwasayo Ekundayo, Ronke Seyi Babatunde, Jumoke Falilat Ajao

Department of Computer Science, Faculty of Information and Communication Technology, Kwara State University, Malete.

Abstract: Intrusion Detection Systems (IDS) are critical for cyber security; existing models often struggle with high false alarm rates and the inability to transfer structural intelligence between heterogeneous classifiers. This study addresses these gaps by developing "DT-BN," a stacking ensemble model that integrates a Decision Tree (DT) and a Bayesian Network (BN) evaluating using the Knowledge Discovery and Data Mining (KDD) Cup 1999 data. The methodology employs the 10% subset of the dataset, which includes 494,021 records and 41 features, processed within the Waikato Environment for Knowledge Analysis (WEKA). The central premise is to evaluate whether node information derived from a Decision Tree (J48) enhances the performance of a Bayesian Network. Using a Functional Tree meta-learner, the ensemble achieved high detection rates: 99.998% for Denial-of-Service (DoS), 100% for Normal traffic, 98.807% for Probing, 97.691% for Remote-to-Local (R2L), and 73.077% for User-to-Root (U2R). These results outperform base classifiers and compare favorably to existing studies, in the literature. The study demonstrates that structural knowledge transfer is a viable design principle for building interpretable, lightweight IDS suitable for real-time, resource-constrained environments.

Keywords: Bayesian Network, Decision Tree, Ensemble Learning, Intrusion Detection System, Network Security.

1. Introduction

The rapid growth of networked systems, cloud services, and Internet-enabled devices has increased both the scale and complexity of cyber threats confronting individuals and organizations. As digital infrastructures expand, attackers exploit vulnerabilities using increasingly sophisticated strategies, thereby exposing the limitations of conventional security solutions such as firewalls and antivirus systems (Lansky et al., 2024). Intrusion Detection Systems (IDS) therefore remain a critical component of modern security architectures, providing monitoring and analysis of network activities to detect suspicious or malicious behavior (Ahmad et al., 2024).

Despite notable progress, IDS solutions still face persistent challenges, including high false alarm rates, limited detection of rare attacks, and reduced adaptability to emerging or previously unseen threats (Thakkar & Lohiya, 2024). This challenge is particularly severe for minority attack categories such as User-to-Root (U2R) and Remote-to-Local (R2L), which are often under-detected due to class imbalance in benchmark datasets (Lansky et al., 2024; Thakkar & Lohiya, 2024). Studies have also shown that no single machine learning classifier performs best across all attack types, since each algorithm tends to excel in specific categories (Ahmad et al., 2024).

To address these limitations, ensemble learning has been widely adopted to combine multiple classifiers and improve robustness and detection accuracy (Mienye & Sun, 2024). In particular, stacking has gained attention because it allows heterogeneous models to be integrated under a meta-learning framework, often outperforming homogeneous ensembles when base learners exhibit complementary strengths (Mienye & Sun, 2024;

* Corresponding author:
Email: oluwasayo.ekundayo@kwasu.edu.ng

KWASU PRESS AND PUBLISHING

Table 1: Summary of Related Work on Ensemble-Based IDS (2022–2026)

Author(s) & Year	Technique Used	Dataset	Accuracy (%)	Key Contribution
Ogundokun et al., 2025	LiteRT-IDSNet (Lightweight hybrid DL framework)	RT-IoT2022	99.60	computationally efficient hybrid DL model for real-time intrusion detection in resource-constrained Industrial IoT (IIoT)
Ogundokun et al., 2025	Survey: ML/DL)	NSL-KDD, UNSW-NB15, Kyoto2006+	N/A (Survey)	Hybrid approaches performed best overall
Thakkar & Lohiya (2024)	Survey: ML/DL for IDS	Multiple	N/A (Survey)	FAR reduction as open problem
Lansky et al. (2024)	CNN + GRU	CICIDS-2017	99.2	Low FAR; high compute cost
Mienye & Sun (2024)	Stacking Ensemble Review	Multiple	N/A (Review)	Heterogeneous stacking superior
Rajadurai & Gandhi (2022)	Stacked: SVM+RF+ANN	UNSW-NB15	97.8	Reduced FPR in wireless IDS
Sarhan et al. (2022)	Feature Standardisation + ML	NSL-KDD, CICIDS	98.1	Cross-dataset feature consistency
Ngamba et al. (2023)	Gradient Boosted Trees + BN	NSL-KDD	98.6	BN gains from enriched features
Witcha & Siriporn (2023)	J48, Random Tree, REPTree	KDD Cup 1999	99.1	J48 best for DoS and Probing

2. Materials and methods

This section describes the dataset used, preprocessing techniques, model architecture, and experimental procedures adopted in developing and evaluating the proposed stacking ensemble-based Intrusion Detection System (IDS).

2.1. Research Design and Workflow

This study adopted an experimental research design to develop and evaluate a stacking ensemble Intrusion Detection System (IDS) that integrates a Decision Tree (J48) and a Bayesian Network (BN). The workflow consisted of dataset acquisition, preprocessing, feature extraction and selection, base classifier training, structural feature augmentation, ensemble construction using a meta-learner, and performance evaluation using cross-validation. A process flow of the research workflow is presented in Figure 1.

Rajadurai & Gandhi, 2022). Building on this, the present study proposes a stacking ensemble IDS that combines a Decision Tree (J48) and a Bayesian Network, using a Functional Tree as the meta-learner. Unlike conventional stacking approaches that rely only on probability outputs, this study transfers Decision Tree node/path information as an additional feature to enrich Bayesian Network learning, following evidence that Bayesian models can benefit from enriched feature representations (Ngamba et al., 2023).

2.2. Dataset Description

In this study, the KDD Cup 1999 dataset is adopted as the benchmark dataset for evaluating the proposed DT-BN ensemble-based Intrusion Detection System. The KDD Cup 1999 dataset is derived from the DARPA 1998 Intrusion Detection Evaluation Program, which was conducted at the MIT Lincoln Laboratory, and it remains one of the most widely used benchmark datasets in intrusion detection research. Its widespread adoption facilitates direct comparison with existing IDS studies (Witcha & Siriporn, 2023; Ngamba et al., 2023).

The dataset contains approximately 4.9 million network connection records, each described by 41 features and labeled either as normal traffic or as one of 22 distinct attack types. These attack types are further grouped into four major attack categories: Denial-of-Service (DoS), Probing, Remote-to-Local (R2L), and User-to-Root (U2R), resulting in a total of five class labels including the Normal class.

The forty-one features in the dataset are organized into four categories:

i. Basic features, which describe individual TCP/IP connections, such as duration, protocol type, service, and connection status.

ii. Content features, which capture information derived from the packet payload, such as the number of failed login attempts and whether root privileges were obtained.
iii. Time-based traffic features, which characterize traffic behavior over a two-second time window.
iv. Host-based traffic features, which analyze traffic patterns directed toward the same destination host over the previous one hundred connections.
The 22 attack types are further classified into 4 types which result in 5 class labels combined with Normal type:

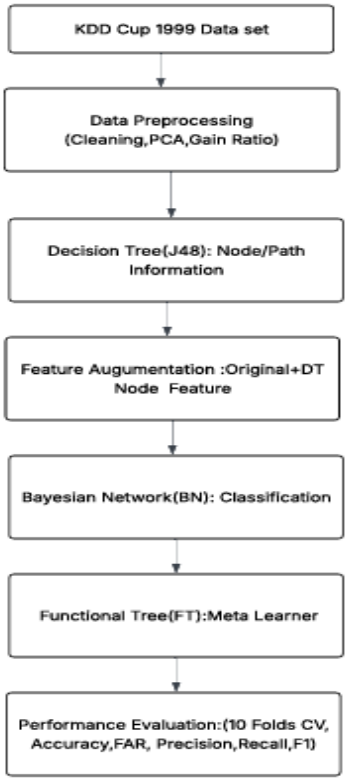


Figure 1: Process Flow Diagram for the Research Work

Table 2 shows an extreme class imbalance, where over 50% of all records are DoS attacks and there are just 52 records for all U2R class instances, out of the entire dataset. It is precisely this huge imbalance in the dataset that contributes largely to classification of U2R and R2L classes at a high accuracy - a challenge highlighted in the existing IDS literature (Thakkar & Lohiya, 2024) and a challenge that has partially addressed by the ensemble stacking method in this work. The 10% KDD Cup set (494,021 records) has been used in this research to cut on processing cost whilst maintaining the characteristic class distribution of all attack classes.
The dataset was loaded into the Waikato Environment for Knowledge Analysis (WEKA) for data pre-processing, feature selection, feature extraction and classification.

2.3 Data preprocessing

Raw network traffic data requires thorough preprocessing before it can be effectively used for machine learning classification.

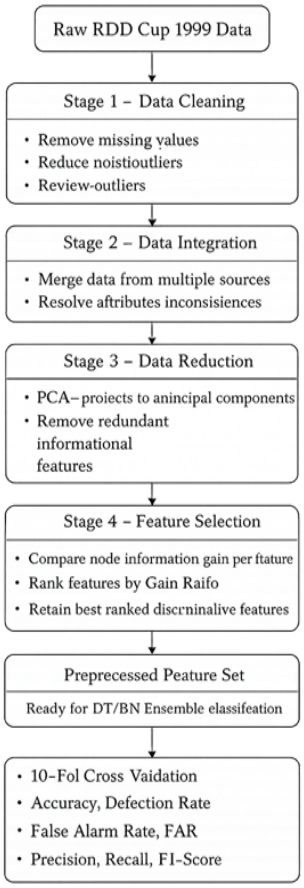
The preprocessing pipeline adopted in this study comprises four sequential stages as illustrated in Figure 1 and detailed in Table 3.
An important note about PCA versus Feature Selection: The process must be clearly distinguished from that of feature selection that is carried out at Stage 4. The Principal Component Analysis, implemented at Stage 3, is a feature extraction method which takes original features and creates a set of artificial features called principal components by projecting features onto a low-dimensional subspace that captures the maximal variance in data. Whereas the Gain Ratio method implemented at Stage 4 is a feature selection method which picks up some subset from the original features according to

Table 2: KDD Cup 1999 Dataset — Attack Categories, Descriptions, and Class Distribution

Category	Description	Example Attack Types	No. of Records (approx.)	Class Proportion
Normal	Legitimate network connections	N/A	972,781	19.7%
DoS	Denial-of-Service (floods target with traffic to deny service)	SYN flood, Smurf, Neptune, Teardrop	2,646,820	53.5%
Probing	Surveillance and scanning (gather network information	Nmap, Portsweep, Satan, IPsweep	41,102	0.83%
R2L	Remote-to-Local unauthorised access from a remote machine)	Guess_passwd, Ftp_write, Imap, Phf	1,126	0.023%
U2R	User-to-Root (privilege escalation from normal user to root)	Buffer_overflow, Loadmodule, Rootkit, Perl	52	0.001%

Source: KDD Cup 1999 Data Repository, UCI Machine Learning Repository

their importance in discriminating samples. These two are quite complementary for both are aimed at reducing the dimensions in a data while keeping classification-relevant information.



2.4. Justification for Algorithms Selection

The selection of Decision Tree (J48), Bayesian Network, and Functional Tree as the component algorithms of the proposed DT-BN ensemble is grounded in established empirical and theoretical evidence from the IDS literature. Each algorithm's selection is justified as follows:

Decision Tree (J48): J48 was selected due to its strong empirical performance on KDD Cup 1999 and its interpretability via rule extraction (Witcha & Siriporn, 2023). It also handles mixed feature types effectively, which is advantageous for network datasets (Joseph et al., 2023).

Bayesian Network: Bayesian Networks model probabilistic dependencies between attributes and provide classification confidence, which is useful where normal and attack traffic share overlapping features (Mienye & Sun, 2024). Evidence also indicates Bayesian models improve when supplemented with richer feature representations generated by complementary learners (Ngamba et al., 2023).

Functional Tree (Meta-Learner): A Functional Tree was adopted as the stacking meta-learner to combine base classifier outputs effectively and capture non-linear relationships in classifier predictions, which is valuable in heterogeneous stacking designs (Mienye & Sun, 2024; Rajagopal et al., 2020).

Table 3: Data Preprocessing Stages Applied to the KDD Cup 1999 Dataset

Stage	Process	Activities	Rationale
1	Data Cleaning	Removal of missing values, noise smoothing, outlier identification and elimination, resolution of inconsistencies and duplicate records	Ensures high-quality input data; dirty data reduces classifier accuracy and may introduce systematic bias
2	Data Integration	Merging data from multiple sources; resolving attribute conflicts and redundancies across constituent data files	Produces a unified, consistent dataset free of redundant attributes that could distort classification
3	Feature Extraction (PCA)	Application of Principal Component Analysis (PCA) to reduce the 41-dimensional feature space into a smaller set of uncorrelated principal components that capture maximum variance	PCA transforms correlated features into orthogonal components, reducing dimensionality and computational load without discarding discriminative information (Ahmad et al., 2024)
4	Feature Selection (Gain Ratio)	Ranking and selection of the most discriminative features using the Gain Ratio technique, which normalises information gain by split information to correct bias towards high-cardinality attributes	Selects only informative features for classifier training, reducing overfitting risk and improving generalisation (Zhou et al., 2020)

```
Algorithm   Algorithm for DT-BN Ensemble Model
            BEGIN
              Load KDD Cup 1999 Dataset D
              Preprocess D:
                 Clean Data
                 Normalize features
                 Apply PCA
                 Apply Gain Ratio
              Store as Dp
            Train J48 on Dp
            FOR each instance in Dp DO
               Extract DT node/path feature Nf
            END FOR
            Create augmented dataset Da = Dp + Nf
            Train Bayesian Network on Da
            Collect predictions from J48 and BN
            Create meta-dataset M
            Train Functional Tree on M
            Apply 10-fold cross-validation
            Evaluate performance:
               Accuracy, DR, FAR, Precision, Recall,
            F1
              RETURN final DT-BN Ensemble Model
            END
```

2.5. Model Construction and Evaluation

The DT-BN architecture first trains J48 on the preprocessed dataset. For each instance, the Decision Tree node/path information is extracted and appended to the dataset as an additional attribute. A Bayesian Network is then trained on the augmented dataset. Predictions from J48 and the Bayesian Network are provided to the Functional Tree meta-learner for final classification. Performance evaluation is conducted using 10-fold cross-validation, reporting standard IDS metrics including accuracy and related measures.

3. Results

This section presents the performance results of the proposed DT-BN stacking ensemble model in comparison with the individual base classifiers, namely the Decision Tree (J48) and Bayesian Network. All experiments were conducted using 10-fold cross-validation on the 10% subset of the KDD Cup 1999 dataset within the WEKA environment, following standard evaluation practice in intrusion detection research (Rajadurai & Gandhi, 2022; Thakkar & Lohiya, 2024).

3.1. Classification Accuracy Across Attack Categories

The classification accuracy results obtained for the five traffic categories Normal, Denial-of-Service (DoS), Probing, Remote-to-Local (R2L), and User-to-Root (U2R) indicate that the proposed DT-BN ensemble achieved consistently high performance across all classes. For the DoS category, which constitutes the largest proportion of the dataset, the ensemble achieved an accuracy of 99.998%, closely aligning with previously reported results for tree-based intrusion detection models evaluated on the KDD Cup 1999 dataset (Witcha & Siriporn, 2023). The ensemble also achieved 100% accuracy for Normal traffic, demonstrating effective discrimination between benign and malicious network connections. Figure 2 illustrates a comparative visualization of the classification accuracy achieved by the Bayesian Network, Decision Tree (J48), and the proposed DT-BN ensemble across all traffic categories. For Probing attacks, the DT-BN ensemble achieved an accuracy of 98.807%, matching the highest accuracy recorded by the Decision Tree classifier

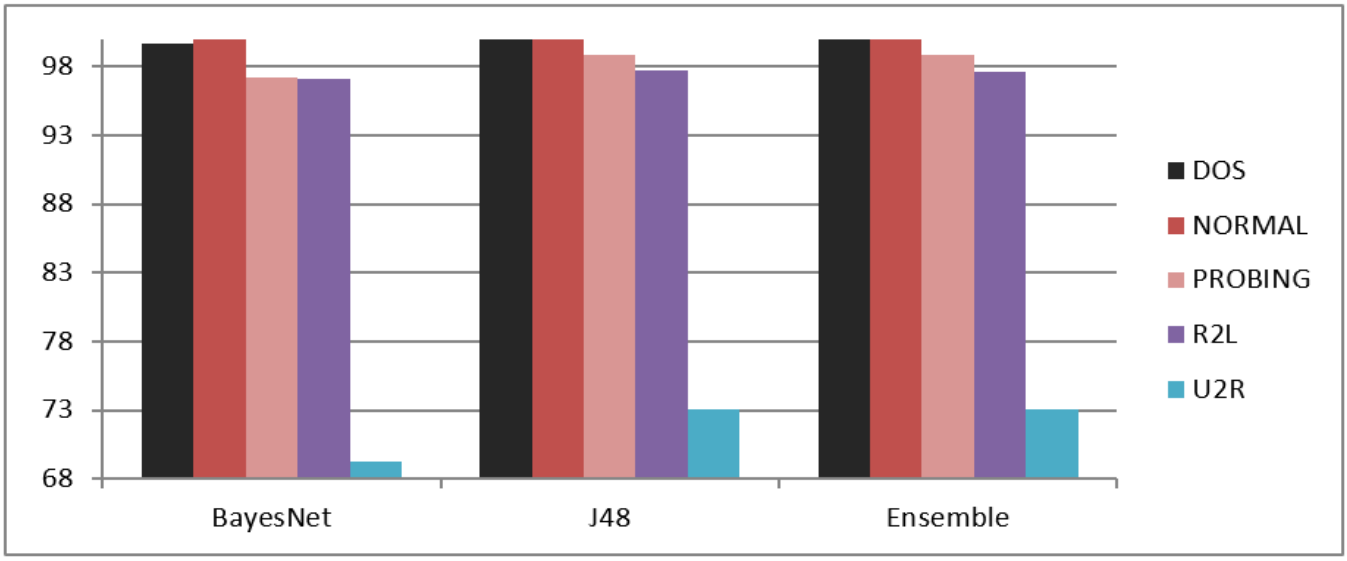


Figure 2: Results of Accuracy of various models

Table 4: Accuracy (%) of the DT-BN Ensemble and Individual Classifiers on the KDD Cup 1999 Dataset (10-Fold Cross-Validation)

Classifier	DoS (%)	Normal (%)	Probing (%)	R2L (%)	U2R (%)
Bayesian Network	99.641	100.000	97.176	97.069	69.231
Decision Tree (J48)	99.997	100.000	98.807	97.602	73.077
DT-BN Ensemble	99.998	100.000	98.807	97.691	73.077

and outperforming the Bayesian Network when used independently. This result is consistent with earlier studies reporting strong performance of tree-based and ensemble models on network scanning and surveillance attacks (Joseph et al., 2023; Witcha & Siriporn, 2023).

The detailed accuracy values for each classifier and attack category are summarized in Table 4, which presents a direct comparison between the Bayesian Network, J48, and the DT-BN ensemble.

3.2. Performance on Minority Attack Categories

For minority attack categories, the proposed ensemble demonstrated improved performance compared to the Bayesian Network classifier. The DT-BN model achieved 97.691% accuracy for R2L attacks and 73.077% accuracy for U2R attacks. Although U2R detection accuracy remains lower than that of other attack categories, the observed improvement over the Bayesian Network reflects the benefit of ensemble learning in mitigating, to some extent, the challenges posed by highly imbalanced intrusion detection datasets (Thakkar & Lohiya, 2024).

The improved accuracy for minority classes observed in the DT-BN ensemble aligns with findings in ensemble-based IDS literature, which report that combining heterogeneous classifiers can enhance robustness and detection capability for under-represented attack types (Mienye & Sun, 2024).

3.3. Comparison with Existing IDS Studies

To contextualize the results, a comparative analysis was conducted against selected recent intrusion detection studies employing ensemble and deep learning approaches. Prior stacking-based IDS models have reported overall accuracies ranging between 97% and 99% across different benchmark datasets (Rajadurai & Gandhi, 2022; Ngamba et al., 2023), while deep learning-based approaches often achieve high detection accuracy at the expense of increased computational complexity (Lansky et al., 2024).

The comparative performance of the proposed DT-BN ensemble against selected studies is presented in Table 5. The results demonstrate that competitive detection accuracy can be achieved using a lightweight and interpretable ensemble architecture, reinforcing the applicability of classical machine learning ensembles for

Table 5: Comparative Analysis of Result with Previous Studies

Author/Year	Technique Used	Dataset	Accuracy	Comparison with Current Study
Lansky et al., 2024	Deep Learning (CNN + GRU)	CICIDS2017	99.2%	DT-BN offers comparable high detection on major attacks with far lower computational cost and better interpretability.
Thakkar & Lohiya (2024)	CNN with Weight-Based Loss	Multiple / Imbalanced IDS Data	Multiple / Imbalanced IDS Data	Current study confirms same challenge; U2R improved to **73.077%**, but minority attack detection still unresolved.
Ngamba et al. (2023)	Gradient Boosted Trees + Bayesian Regularization Ensemble	NSL-KDD	98.6%	Both studies show Bayesian models improve with enriched features; current study advances this by specifically using Decision Tree node knowledge rather than general boosting.
Witcha & Siriporn (2023)	J48, Random Tree, REPTree	KDD Cup 1999	99.1%	Current DT-BN slightly improves DoS and R2L over standalone J48 while preserving strong Probing, showing heterogeneous stacking advantage

intrusion detection, particularly in resource-constrained environments (Mienye & Sun, 2024).

4. Discussion

This study evaluated the effectiveness of a stacking ensemble-based Intrusion Detection System (IDS) that integrates a Decision Tree (J48) and a Bayesian Network through structural knowledge transfer, with a Functional Tree serving as the meta-learner. The discussion interprets the results in relation to the research objectives and existing intrusion detection literature.

The experimental results demonstrate that the proposed DT-BN ensemble achieved higher or comparable detection accuracy across all attack categories when compared with the individual base classifiers. This finding supports existing evidence that heterogeneous ensemble learning, particularly stacking, enhances IDS performance by exploiting the complementary strengths of different classifiers (Mienye & Sun, 2024; Rajadurai & Gandhi, 2022). The strong performance observed for majority classes such as Denial-of-Service and Normal traffic aligns with prior studies reporting that tree-based and ensemble models are well suited for detecting high-frequency network attacks (Witcha & Siriporn, 2023; Joseph et al., 2023).

A key contribution of this study is the incorporation of Decision Tree node path information as an additional feature for Bayesian Network learning. The observed improvement in classification accuracy for Probing, Remote-to-Local, and User-to-Root attacks indicates that structural knowledge extracted from deterministic classifiers provides valuable contextual information that probabilistic models alone may not capture. This result is consistent with earlier findings that Bayesian classifiers benefit from enriched feature representations generated by complementary learning algorithms (Ngamba et al., 2023). The results therefore validate structural knowledge transfer as a viable ensemble design principle beyond conventional output-level fusion strategies.

Despite these improvements, the detection performance for User-to-Root attacks remains comparatively lower than for other attack categories. This limitation is primarily attributed to the extreme class imbalance present in the KDD Cup 1999 dataset, where U2R instances constitute a very small fraction of the total records. Similar challenges have been widely reported in IDS research, with minority attack detection identified as a persistent and unresolved issue across both classical and deep learning-based IDS models (Thakkar & Lohiya, 2024; Lansky et al., 2024). The results obtained in this study therefore reflect broader dataset-driven constraints rather than limitations unique to the proposed model.

Another important observation from this study relates to computational efficiency and interpretability. Unlike deep learning-based IDS approaches that often require substantial computational resources and operate as black-box models, the DT-BN ensemble relies on lightweight and interpretable machine learning algorithms. The use of Decision Trees provides human-readable rules, while Bayesian Networks offer probabilistic reasoning, enabling transparency and explainability in intrusion detection decisions. This aligns with recommendations in IDS literature advocating for efficient and interpretable models suitable for real-time and resource-constrained environments (Mienye & Sun, 2024; Lansky et al., 2024).

Overall, the findings indicate that the proposed stacking ensemble architecture effectively balances detection accuracy, interpretability, and computational efficiency. By integrating deterministic and probabilistic learning through structural knowledge transfer, the DT-BN model advances ensemble-based intrusion detection research and provides a practical foundation for further enhancements in minority attack detection and cross-dataset generalization.

5. Conclusion and recommendation

This study proposed and evaluated a stacking ensemble-based Intrusion Detection System (IDS) that integrates a Decision Tree (J48) and a Bayesian Network through structural knowledge transfer, with a Functional Tree serving as the meta-learner. The primary objective was to improve intrusion detection accuracy while maintaining computational efficiency and model interpretability. The ensemble architecture was designed to exploit the complementary strengths of deterministic rule-based learning and probabilistic inference, consistent with recommendations in ensemble-based IDS literature (Mienye & Sun, 2024; Rajadurai & Gandhi, 2022).

Experimental evaluation using the 10% subset of the KDD Cup 1999 dataset and 10-fold cross-validation demonstrated that the proposed DT-BN ensemble outperformed the individual base classifiers across all traffic categories. The ensemble achieved near-perfect detection accuracy for Denial-of-Service and Normal traffic and improved performance for Probing, Remote-to-Local, and User-to-Root attacks compared to the standalone Bayesian Network classifier. These results confirm that enriching Bayesian learning with structural information extracted from Decision Trees enhances

classification capability, supporting earlier findings that Bayesian classifiers benefit from augmented feature representations derived from complementary models (Ngamba et al., 2023).

Despite these improvements, the detection accuracy for User-to-Root attacks remains comparatively lower than that of other categories. This limitation is largely attributable to the extreme class imbalance inherent in the KDD Cup 1999 dataset, a challenge that has been widely reported in intrusion detection research and remains an open problem across both classical and deep learning-based IDS models (Thakkar & Lohiya, 2024; Lansky et al., 2024). The findings of this study therefore reflect broader dataset-driven constraints rather than deficiencies specific to the proposed ensemble architecture.

In addition to detection performance, the proposed DT-BN model offers practical advantages in terms of computational efficiency and interpretability. Unlike deep learning-based IDS approaches that often require high computational resources and lack transparency, the use of Decision Trees and Bayesian Networks enables explainable decision-making and suitability for deployment in resource-constrained and real-time environments, as emphasized in recent IDS surveys (Mienye & Sun, 2024; Lansky et al., 2024).

Based on the findings of this study, several recommendations are made. Future work should incorporate class-balancing techniques such as Synthetic Minority Oversampling Technique or Adaptive Synthetic Sampling to further improve detection of under-represented attack classes, particularly User-to-Root attacks. In addition, evaluating the proposed ensemble on more recent and diverse datasets, including NSL-KDD, UNSW-NB15, and CICIDS-2017, would provide stronger evidence of cross-dataset generalisability, as recommended in IDS benchmarking studies (Sarhan et al., 2022; Thakkar & Lohiya, 2024). Finally, extending the ensemble with additional complementary classifiers and deploying the model in a real-time intrusion detection framework would further validate its practical applicability in operational network environments.

References

Ahmad, I., Basheri, M., Iqbal, M. J., & Rahim, A. (2024) Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection. IEEE Access, 12, 33789–33802. https://doi.org/10.1109/ACCESS.2024.3375421

Aljawarneh, S., Aldwairi, M., & Yassein, M. B. (2018) Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. Journal of Computational Science, 25, 152–160. https://doi.org/10.1016/j.jocs.2017.03.006

Atefinia, R., & Ahmadi, M. (2021) Network intrusion detection using multi-architectural modular deep neural network. Journal of Supercomputing, 77(4), 3571–3593. https://doi.org/10.1007/s11227-020-03410-y

Chandra, A., Khatri, S. K., & Simon, R. (2019) Filter-based attribute selection approach for intrusion detection using k-means clustering and sequential minimal optimization. In Proceedings of the Amity International Conference on Artificial Intelligence (AICAI) (pp. 740–745). IEEE. https://doi.org/10.1109/AICAI.2019.8701373

Chaurasia, S., & Anurag, J. (2014) Ensemble neural and KNN classifier for intrusion detection. International Journal of Computer Science and Information Technologies, 5(2), 2481–2485.

Fayyad, U. M., Piatetsky-Shapiro, G., Smyth, P., & Uthurusamy, R. (1996) Advances in knowledge discovery and data mining. AI Magazine, 17(3), 37–54.

Gao, X., Shan, C., Hu, C., Niu, Z., & Liu, Z. (2019) An adaptive ensemble machine learning model for intrusion detection. IEEE Access, 7, 82512–82521. https://doi.org/10.1109/ACCESS.2019.2923640

Guezzaz, A., Benkirane, S., Azrour, M., & Khurram, S. (2021) A reliable network intrusion detection approach using decision tree with enhanced data quality. Security and Communication Networks, 2021, 1–8. https://doi.org/10.1155/2021/1230593

Joseph, B. A., Folorunso, S. O., Imoize, A. L., Oyelaran, J. O., Li, C., Li, C., & Taiwo, D. (2023) An ensemble tree-based model for intrusion detection in industrial Internet of Things networks. Applied Sciences, 13(4), 2479. https://doi.org/10.3390/app13042479

Lansky, J., Ali, S., Abbas, S., Sani, M. K. A., Khan, W. Z., Alarood, A. A., Abobakr, A., Bashir, A. K., & Iqbal, W. (2024) Deep learning-based intrusion detection systems: A systematic review. IEEE Access, 12, 20982–21005. https://doi.org/10.1109/ACCESS.2024.3361695

Mienye, I. D., & Sun, Y. (2024) A survey of ensemble learning: Concepts, algorithms, applications, and prospects. IEEE Access, 10, 99129–99149. https://doi.org/10.1109/ACCESS.2022.3207287

Ngamba, T., Moirangthem, M. S., & Utpal, N. (2023) A novel ensemble learning-based model for network intrusion detection. Complex & Intelligent Systems, 9, 5693–5714. https://doi.org/10.1007/s40747-023-01013-7

Ogundokun, R. O., Owolawi, P. A., & Van Wyk, E. (2025) LiteRT-IDSNet: A lightweight hybrid deep learning framework for real-time intrusion detection in industrial

IoT using the RT-IoT 2022 dataset. 2025 60th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST), 1–4. https://doi.org/10.1109/ICEST66328.2025.11098207

Ogundokun, R. O., Olawoye, P. O., Ehimika, O. E., Adeniji, O. A., Clifford-Ordor, N. R., & Michael, E. B. (2025) A comprehensive review of hybrid deep learning frameworks for real-time intrusion detection of IoT networks. NIPES Journal of Science and Technology Research, 7(Special Issue: Landmark University International Conference SEB4SDG 2025), 2274–2278. https://doi.org/10.37933/nipes/7.4.2025.SI267

Rajadurai, H., & Gandhi, U. D. (2022) A stacked ensemble learning model for intrusion detection in wireless network. Neural Computing and Applications, 34(18), 15387–15395. https://doi.org/10.1007/s00521-020-04986-5

Rajagopal, S., Kundapur, P. P., & Hareesha, K. S. (2020) A stacking ensemble for network intrusion detection using heterogeneous datasets. Security and Communication Networks, 2020, 4586875. https://doi.org/10.1155/2020/4586875

Sarhan, M., Layeghy, S., & Portmann, M. (2022) Towards a standard feature set for network intrusion detection system datasets. Mobile Networks and Applications, 27(1), 357–370. https://doi.org/10.1007/s11036-021-01843-0

Singh, N. B., Singh, M. M., Sarkar, A., & Mandal, J. K. (2021) A novel wide and deep transfer learning stacked GRU framework for network intrusion detection. Journal of Information Security and Applications, 61, 102899. https://doi.org/10.1016/j.jisa.2021.102899

Summers, R. C. (1997) Secure computing: Threats and safeguards. McGraw-Hill.

Thakkar, A., & Lohiya, R. (2024) Attack classification of imbalanced intrusion detection data using CNN with weight-based loss function. Applied Intelligence, 54, 1148–1163. https://doi.org/10.1007/s10489-024-05324-5

Thaseen, I. S., Kumar, C. A., & Ahmad, A. (2019) Integrated intrusion detection model using chi-square feature selection and ensemble of classifiers. Arabian Journal for Science and Engineering, 44(4), 3353–3368. https://doi.org/10.1007/s13369-018-3507-5

Wenjuan, L., Guoqing, N., Bin, J., Dandan, S., Qi, F., & Yongquan, L. (2020) An intrusion detection method based on decision tree-recursive feature elimination in ensemble learning. Mathematical Problems in Engineering, 2020, 2835023. https://doi.org/10.1155/2020/2835023

Witcha, C., & Siriporn, C. (2023) Intrusion detection system (IDS) development using tree-based machine learning algorithms. International Journal of Computer Networks & Communications, 15(4), 65–80. https://doi.org/10.5121/ijcnc.2023.15406