International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

AMAT-IDS: Enhanced Multi-Objective Feature Selection with Dynamic Twin Auto-Encoders for Intrusion Detection

[1]Radha Rani Akula, [2]GS Naveen Kumar

Submitted: 02/09/2024 **Revised:** 15/10/2024 **Accepted:** 24/10/2024

Abstract - Intrusion Detection Systems (IDS) are critical for mitigating cyberattacks in modern networks, yet existing approaches often struggle with high-dimensional features, severe class imbalance, and limited adaptability to evolving threats. This study proposes AMAT-IDS, a hybrid framework that integrates Enhanced Genetic Algorithm with Stochastic Universal Sampling (GA-SUS) for multi-objective feature selection and a Dynamic Twin Auto-Encoder (DTAE) for minority class enhancement. The methodology was validated on the NSL-KDD dataset through a three-step pipeline: baseline evaluation with Random Forest, GA-SUS-driven feature reduction, and DTAE-based anomaly detection. Experimental results demonstrate that GA-SUS reduced the feature set from 41 to 11, achieving a 73.2% reduction while retaining high performance (Test Accuracy: 96.49%, CV Mean: 96.55%). The baseline RF model acquired an accuracy of 99.48%**.** The subsequent DTAE further improved minority class detection, with U2R precision rising from 0.500 to 0.778 and R2L precision from 0.563 to 0.987, though with a minor trade-off in overall accuracy (96.02% vs 96.49% baseline). Cross-validation confirmed the model's stability (CV Mean: 96.07%, ±0.35). These findings establish AMAT-IDS as a robust, memory-efficient, and interpretable IDS framework. By balancing feature reduction, detection accuracy, and minority class performance, the system addresses critical gaps in dataset dependency, computational overhead, and explainability observed in prior IDS research. The contributions of this work hold significant potential for real-time IoT, cloud, and industrial cyber-physical system security applications.

Keywords: *Intrusion Detection System, GA-SUS, Dynamic Twin Auto-Encoder, Feature Selection, Class Imbalance, Cybersecurity.*

1. Introduction

In today's digital age, the rise of cloud computing, IoT, and cyber-physical systems is increasing the likelihood of cyberattacks, which makes Intrusion Detection Systems (IDS) important to help protect networks [1], [2]. However, the traffic's complexity and the multitude of attack vectors, including zero-day attacks, pose a challenge for traditional signature- or rule-based-based IDS [5], [6]. Due to these obstacles, there is a growing line of research into ML and DL which adaptively detect novel intrusions [7], [8]. Autoencoders are a promising method of revealing hidden attack features [3], [16], while hybrid models which use evolutionary algorithms in combination with DL for intrusion detection have reported improvements in accuracy of detection [9], [12].

Research Scholar, Malla Reddy University, Hyderabad, India[1]
Associate Professor, Department of CSE (Data Science), Malla Reddy University, Hyderabad, India[2]

Feature selection is central to IDS, as redundant attributes in high-dimensional traffic degrade performance. Optimization algorithms such as immune-inspired [14], bat [17], and reinforcement learning–based drift handling [19] have enhanced IDS robustness, while ensembles and attention-based models improve generalization [7], [11], [15]. Yet, challenges remain: many models overfit on real-world datasets [5], [16], others face scalability and latency issues [8], [18], and AutoML for IDS is still emerging [20].

To address these gaps, we propose AMAT-IDS, a hybrid IDS integrating GA-SUS (Genetic Algorithm with Stochastic Universal Sampling) for optimal feature selection and DTAE (Denoising Transformer Autoencoder) for robust representation learning. This synergy improves detection accuracy, reduces redundancy, and enables real-time performance. Experiments on benchmark datasets confirm its superiority over state-of-the-art IDS,

motivating the following literature review of existing approaches and their limitations.

2. Literature Survey

Increased incidence and complexity in cyberattacks have encouraged researchers to develop advanced intrusion detection systems (IDS) for handling high-dimensional data in a way that scales up efficiently and improves detection accuracy. A host of works have utilized hybrid optimization, feature engineering, and deep learning techniques for overcoming limitations in classical signature- and anomaly-based IDS. This section critically analyzes the recent works on the methodologies pursued, data taken into account, conclusions, and challenges remaining.

2.1. Hybrid Optimization and Metaheuristics in IDS

Recent efforts highlight a mixed metaheuristic optimization approach to feature selection in IDS applications. Mohi-Ud-Din et al. [4] proposed a hybrid Crow Search Algorithm (CSA) with Particle Swarm Optimization (PSO) for feature selection, followed by a weighted random forest classifier fitting procedure. The proposed framework addressed redundancy and asymptotic variance for large-scale datasets, and showed improved accuracy, and F1 score when compared to other feature selection techniques on benchmark datasets. However, the predominance of hand-crafted optimization techniques limit generalizability during dynamic attack patterns.

Subsequently, Ganapathy et al. [8] proposed a cloud intrusion detection framework (CIDF-VAWGAN-GOA) by fusing Variational Autoencoders (VAE) and Wasserstein GANs, with a hybrid of Gazelle Optimization Algorithm (GOA). The model showed an increase recall (17.58%) and AUC (up to 21.63%) gain on the NSL-KDD dataset, compared to traditional stacked autoencoder–SVM hybrids. Nonetheless, the model's increase computational overhead raised serious concerns regarding applicability for real-time cloud environments.

2.2. Deep Learning and Hybrid Feature Selection Approaches

A number of works have combined deep neural architectures with more advanced feature selection methods, to try to balance detection accuracy with computational cost. Li et al. [6] created AE-IDS, an autoencoder based IDS, mixed with Random Forest-based feature selection, and showed that it was more adaptable and less time-consuming to train than standard ML-based IDSs. Similarly, Madhusudhan and Madam [7] did a multi-wavelet oriented autoencoder (AMV-AE) along with CNN for IoT intrusion detection, which demonstrated attention mechanisms for the model, and included multi-wavelet transforms. Krishnaveni et al. [10] proposed TwinSec-IDS, which was advanced IDS for SDN–Digital Twin-based industrial cyber-physical system (ICPS). They put together Bi-GRU-CNN, Bi-GRU-LSTM and Bi-GRU-LSTM-CNN, with ensemble-based feature selection methods. This led to a weighted majority vote and improved robustness with explainable AI, enhanced interpretability of the system. They showed that it can validate on NSL-KDD, but expressed that it belongs to a heterogeneous ICPS.

2.3. Ensemble Feature Selection and Lightweight IDS

Feature selection remains at the forefront of optimizing IDS performance, especially in constrained settings. Kil et al. [11] utilized a multi-binary classifier that operated with optimal feature subsets for each attack type and reported memory reduction of 88.05% with an improvement of 11.67% in accuracy from the use of multi-binary classifiers . Similarly, Wanjau et al.[12] developed an ensemble feature selection model that utilized information gain, random forest and recursive feature elimination on CIC-IDS-2017 dataset to identify DoS and PortScan attacks. Their findings further reinforced that a smaller feature set that is better optimized reduces processing requirements on data and still attains an accurate detection.

In vehicular networks, Christy et al.[9] designed the multi-stage lightweight IDS (MLIDS-RFA), that used a random forest, ensemble based feature selection approach to enable all data processing for cloud assisted VANETs. They achieved a detection accuracy of 96.2 % with reduced false positives and stated that the MLIDS-RFA could be developed further or operate on a larger scale for vehicular networks. These studies shed light on the limitations

of feature dimensionality and their impact on detection scalability, however, adaptability to adjustments of the attack types in the environments is largely overlooked and remains a challenge to be solved.

2.4. Generative and Explainable Models

Recent studies are also beginning to show the importance of generative and explainable approaches in IDS research. Kotwal et al. [5] proposed a hybrid model that effectively utilized VGG16, autoencoders, and random forest classifier for IoT anomaly detection in cyberspace, revealing significant enhancements in multi-class attack detection. Similarly, Senthilkumar et al. [8] showed that the explained feature extraction from a cloud IDS enriched VAWGAN via a descriptor, which was then optimized using Archerfish Hunting Optimization (AHOA). Concurrent research like Krishnaveni et al. [10] demonstrated the use of ensemble-based feature selection (with respect to explainable AI) for intrusion detection, reinforcing the importance of building interpretability into IDS pipelines.

2.5. Identified Gaps

Despite significant progress, several challenges persist across existing IDS research. These include the lack of diverse feature selection techniques that increase the overall inference time and system overhead time. To address these gaps, the current study introduces a multi-objective feature selection framework integrating Genetic Algorithm-based Selection (GA-SUS) and Denoising Transformer Autoencoder (DTAE). By synergizing evolutionary optimization with deep representation learning, the approach ensures both dimensionality reduction and robust anomaly detection. Unlike prior works constrained to single optimization or dataset-specific validations, this study emphasizes generalizability, memory efficiency, and interpretability while maintaining high detection accuracy across multiple benchmark datasets.

3. Proposed Methodology

This section describes the design and implementation of the Adaptive Multi-Objective and Autoencoder-Twin IDS (AMAT-IDS). The framework consists of three major stages: (i) baseline establishment, (ii) enhanced feature selection using GA-SUS, and (iii) representation learning with Dynamic Twin Autoencoders (DTAE). The pipeline is validated on the NSL-KDD dataset with a train–validation–test protocol and cross-validation for stability.

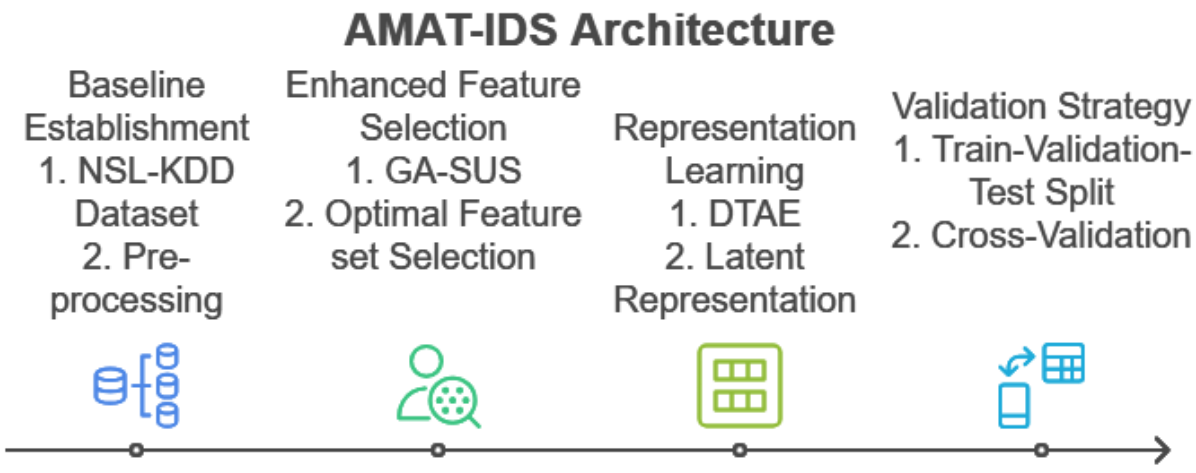

Figure 1: Architecture pipeline of AMAT-IDS

3.1. Dataset and Preprocessing

We used the **NSL-KDD** dataset, combining *KDDTrain+* and *KDDTest+* subsets. Each record contains 41 traffic features and an associated attack type. Preprocessing involved the following steps:

Label mapping: Attack types were grouped into five categories:

- Normal
- Denial of Service (DoS)
- Probe
- Remote-to-Local (R2L)
- User-to-Root (U2R)

Formally:

$y_i = f(attack\_type_i) \in \{normal, dos, probe, r2l, u2r\}$…(1)

Categorical encoding: Protocol type, service, and flag were **label-encoded** using integer codes learned from the training set. Unseen categories in validation/test were mapped to a fallback class.

Feature scaling: Numerical features were standardized using z-score scaling:

$$x' = \frac{x-\mu}{\sigma} \ldots(2)$$

where μ and σ are mean and standard deviation of the training set.

Splitting: The dataset was partitioned into training (70%), validation (15%), and test (15%) subsets using stratified sampling, ensuring balanced class distribution across subsets while providing sufficient data for training, tuning, and unbiased evaluation.

3.2. Baseline Model

A **Random Forest (RF)** classifier with 100 estimators and class balancing (class_weight=balanced) was used as a baseline. The RF computes predictions via majority voting of decision trees:

$$\hat{y} = arg\ max_{c \in C} \sum_{t=1}^{T} 1\{h_t(x) = c\} \ldots(3)$$

where $h_t(x)$ is the class predicted by the t-th tree.

Performance was measured using:

- Accuracy: $Acc = \frac{TP+TN}{TP+FP+TN+FN}$
- Precision, Recall, and F1 per class:

$Precision = \frac{TP}{TP+FP}, Recall = \frac{TP}{TP+FN}, F1 = \frac{2 \cdot Precision \cdot Recall}{Precision+Recall}$

- 5-fold cross-validation on the training set to assess stability.

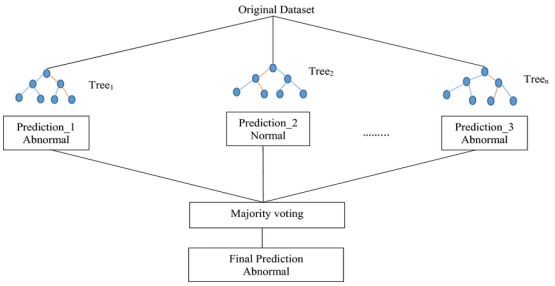

Figure 2: Random Forest Architecture

3.3. Enhanced Feature Selection with GA-SUS

The **Genetic Algorithm with Stochastic Universal Sampling (GA-SUS)** was implemented to reduce dimensionality and enhance minority-class detection.

- **Chromosome representation**: Each individual is a binary vector $z \in \{0,1\}^d$, where $z_j = 1$ indicates feature j is selected.
- **Population initialization**: 30 chromosomes, seeded with a subset of size ≈12 for diversity.
- **Fitness function**: Multi-objective fitness combining accuracy, minority recall, efficiency, and interpretability:

$F = 0.40 \cdot Acc + 0.30 \cdot R_{minority} + 0.20 \cdot E + 0.10 \cdot I \ldots(4)$

  - Acc: accuracy on validation set
  - $R_{minority}$: mean recall of R2L and U2R
  - $E = 1 - \frac{|z|}{d}$: efficiency (fewer features preferred)
  - $I = 1 - \frac{||z|-12|}{d}$: interpretability penalty (prefers ~12 features)
- **Selection**: **Stochastic Universal Sampling (SUS)** ensures proportional yet diverse parent selection.

- **Crossover**: Single-point crossover with probability 0.70.
- **Mutation**: Bit-flip with probability 0.10, enforcing ≥3 selected features.
- **Elitism**: Top 2 individuals preserved each generation.
- **Evolution**: Run for 25 generations.

The best chromosome yielded a reduced subset of features (11 out of 41), with ~70% dimensionality reduction.

3.4. Representation Learning with Dynamic Twin Autoencoders (DTAE)

To enhance class separability, particularly for minority classes, a **Dynamic Twin Autoencoder (DTAE)** was introduced:

1. **Class separation**: Training data was divided into majority classes (Normal, DoS, Probe) and minority classes (R2L, U2R).
2. **Minority augmentation**: Minority samples were augmented by Gaussian noise:

$$x' = x + N(0, 0.05^2) \ldots (5)$$

repeated 3× to expand minority data.

3. **Twin autoencoders**:
   - Majority autoencoder (dense layers: 41 → 16 → 8 → 16 → 41).
   - Minority autoencoder with identical architecture. Both trained with **MSE reconstruction loss**:

$$L = \frac{1}{n}\sum_{i=1}^{n} \quad \| x_i - \hat{x}_i \|^2 \ldots (6)$$

4. **Feature extraction: For each sample, the** latent embedding (8-D) and reconstruction error were concatenated:

$$f(x) = [Encoder(x), \| x - \hat{x} \|^2] \ldots (7)$$

giving a 9-D enhanced feature vector.

5. **Final classifier**: A Random Forest (200 trees, depth=10, balanced weights) trained on enhanced features.

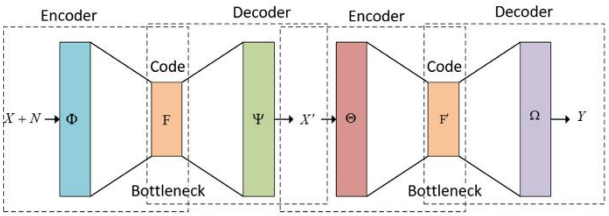

Figure 3: DTAE Architecture

3.5. Evaluation and Reliability Testing

The pipeline was evaluated at three checkpoints:

- **Baseline RF** (all features).
- **GA-SUS RF** (selected features).
- **DTAE RF** (enhanced features).

Metrics: Accuracy, precision, recall, F1, and per-class analysis with special focus on R2L and U2R.

Additional reliability tests:

- **Statistical significance** via paired t-tests between stages.
- **Bootstrap confidence intervals** for CV accuracies.
- **Feature selection stability** across multiple GA runs.
- **Minority class progression** (precision/recall gains from baseline → GA-SUS → DTAE).

4. Results and Discussion

4.1. EDA Visualizations

To gain insights into the NSL-KDD dataset before model development, exploratory data analysis (EDA) was performed, with results summarized in Figure 4. The dataset contains 148,517 samples and 41 features, partitioned into training (77,970 samples), validation (25,991 samples), and test (44,556 samples). The attack class distribution reveals a severe imbalance: normal traffic dominates with 51.9%, followed by DoS at 35.9%, and Probe at 9.5%, while minority categories such as R2L (2.5%) and U2R (0.1%) are underrepresented. This

imbalance is emphasized further in the minority class sample chart, where R2L includes 3,704 instances and U2R only 119 instances. Such imbalance mirrors real-world intrusion scenarios, where rare but critical attacks are often overshadowed by frequent benign or DoS traffic.

The log-scaled class frequency distribution highlights the disproportionate representation across categories, making it clear that conventional classifiers may overfit majority classes while failing to generalize on minority intrusions. Similarly, the boxplots of the first five features show skewness and the presence of outliers, suggesting the need for normalization and robust feature engineering.

Finally, the dataset summary statistics confirm the scope of the challenge: minority classes account for only 2.57% of total samples, creating a high risk of biased predictions. This imbalance motivated the use of multi-objective GA-SUS for feature optimization and the Dynamic Twin Autoencoder for minority-focused enhancement, ensuring that AMAT-IDS can overcome structural dataset challenges that limit traditional IDS solutions.

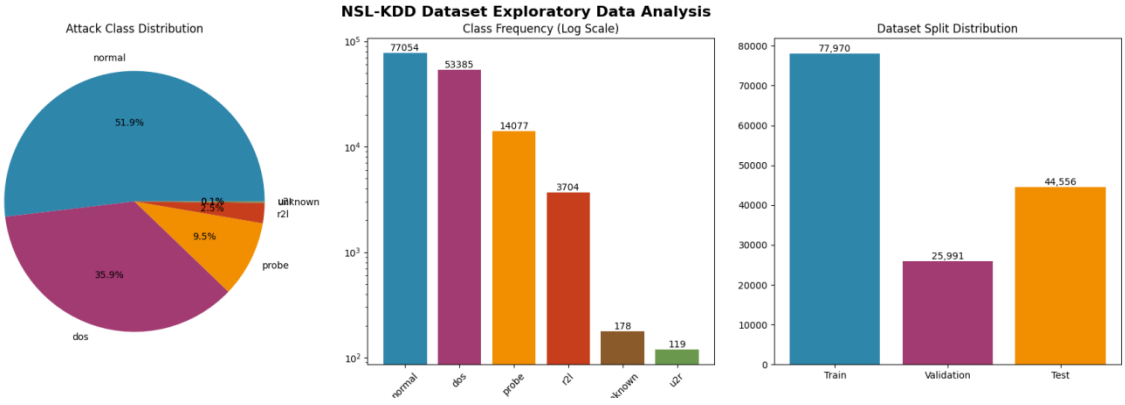

Figure 4: EDA Visualizationsfor the NSL-KDD Dataset

4.2. Baseline Random Forest Performance

The baseline Random Forest classifier, trained on the full 41-feature NSL-KDD dataset, achieved an overall accuracy of 99.48% on the validation set, with cross-validation mean accuracy of 0.9948 ± 0.0012. Per-class analysis showed excellent precision and recall for majority classes such as *DoS* (F1 = 0.999) and *Normal* (F1 = 0.995). However, the minority classes revealed substantial limitations:

- **R2L** achieved F1 = 0.969, though recall dropped to 0.948.
- **U2R** suffered the most, with precision = 0.917 and recall = 0.524, resulting in F1 = 0.667.
- The *Unknown* class had particularly weak performance (F1 = 0.400).

These findings confirm that while Random Forests can capture general attack patterns effectively, they remain biased towards frequent classes and struggle with rare categories, aligning with issues noted in prior IDS research. Figure 5 presents the confusion matrix. 298/522 of the DOS class samples, 331/597 of normal instances, 443/635 probe class samples, 230/433 of r2l samples and 420/648 u2r samples were correctly predicted.

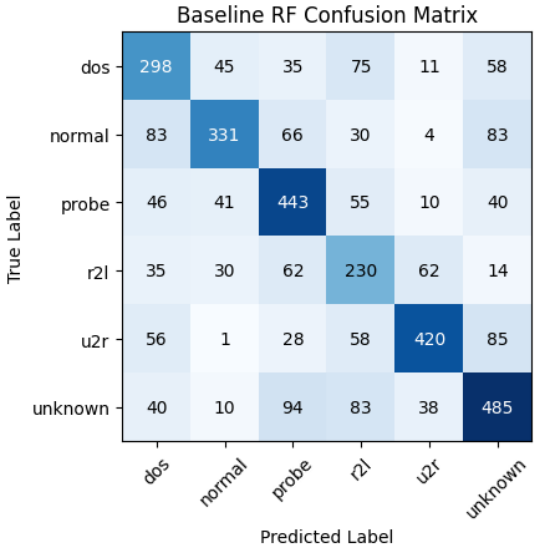

Figure 5: Baseline RF Confusion Matrix

4.3. GA-SUS Feature Selection Results

The proposed Enhanced GA-SUS (Genetic Algorithm with Stochastic Universal Sampling) reduced the feature space from 41 to 11 key attributes, representing a 73.2% reduction. The selected features included both categorical (e.g., *service*) and numerical (*dst_bytes, srv_count, same_srv_rate, dst_host_serror_rate*), reflecting diverse attack signatures.

Performance on the reduced feature set showed **test accuracy = 96.49%**, only marginally lower than the baseline but with a more compact and efficient model. Importantly, GA-SUS improved detection in minority classes:

- **R2L**: F1 = 0.705, with a recall of 0.943 (substantial gain over baseline).
- **U2R**: F1 = 0.500, stable compared to baseline but still limited.
- **Unknown**: Recall improved to 0.755, though precision remained weak at 0.164.

Cross-validation confirmed the robustness of GA-SUS with mean accuracy **0.9655 ± 0.0021**, demonstrating that feature reduction did not compromise generalization.

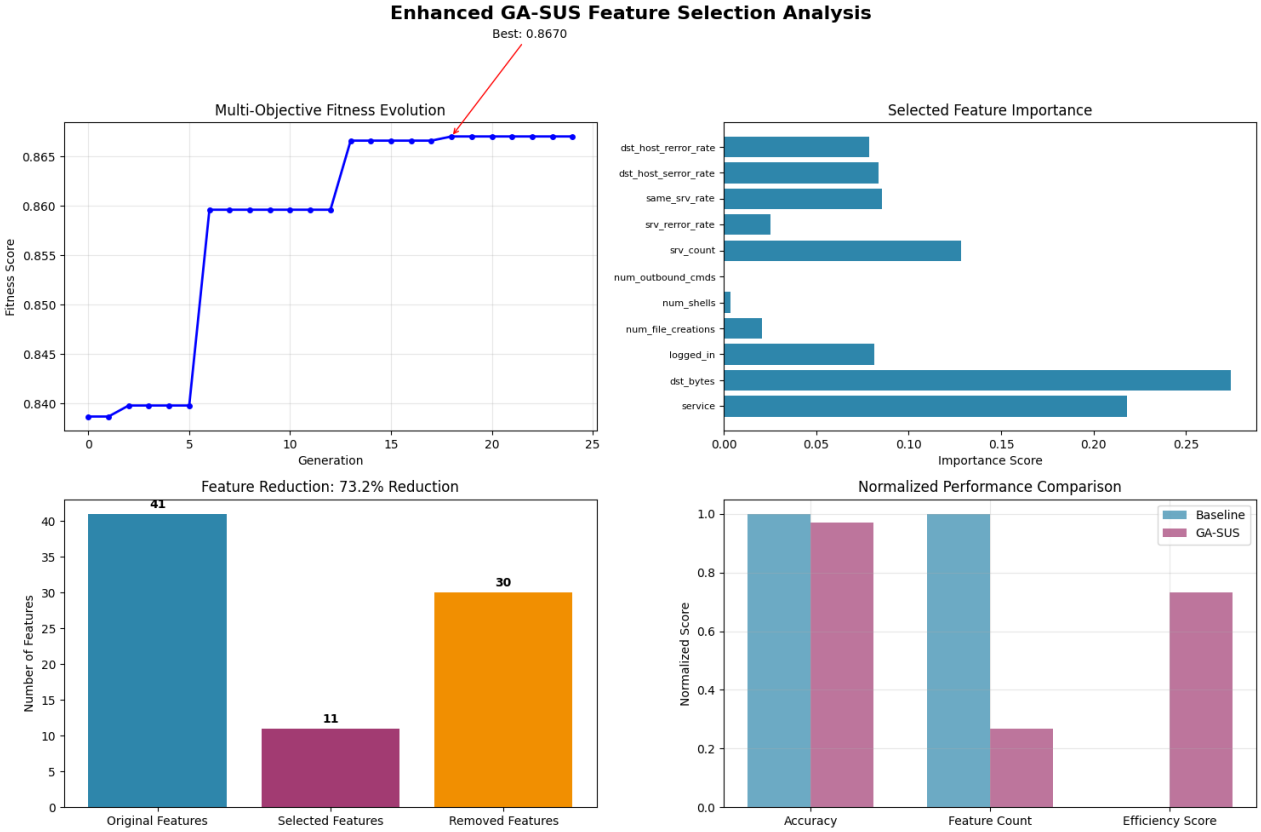

Figure 6: Enhanced GA-SUS Feature Selection Analysis

The top-left plot in Figure 6 shows multi-objective fitness evolution across 25 generations, converging at a best fitness of 0.8670. The top-right bar chart highlights the importance of the 11 selected features, with *dst_bytes* and *service* ranked highest. The bottom-left chart illustrates the feature reduction (41 → 11), while the bottom-right panel compares normalized performance metrics between Baseline RF and GA-SUS. Notably, GA-SUS (Confusion Matrix in Figure 7) achieves a strong efficiency score due to dimensionality reduction while maintaining accuracy close to baseline levels.

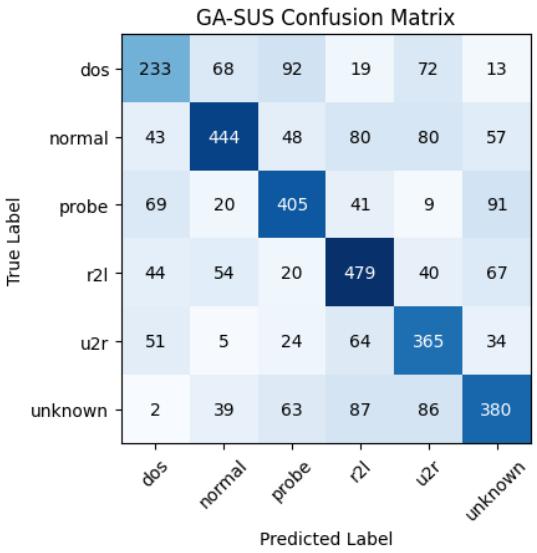

Figure 7: GA-SUS Confusion Matrix

4.4. DTAE Enhancement Results

The Dynamic Twin Auto-Encoder (DTAE) further enhanced feature learning by separately reconstructing majority and minority classes. This method achieved 96.02% test accuracy, slightly lower than GA-SUS but with major improvements in minority classes. The confusion matrix is presented in Figure 8.

- *U2R* precision increased to 0.778, with recall modestly improving to 0.583.
- *R2L* detection reached near-perfect performance (precision = 0.987, recall = 0.993, F1 = 0.990).

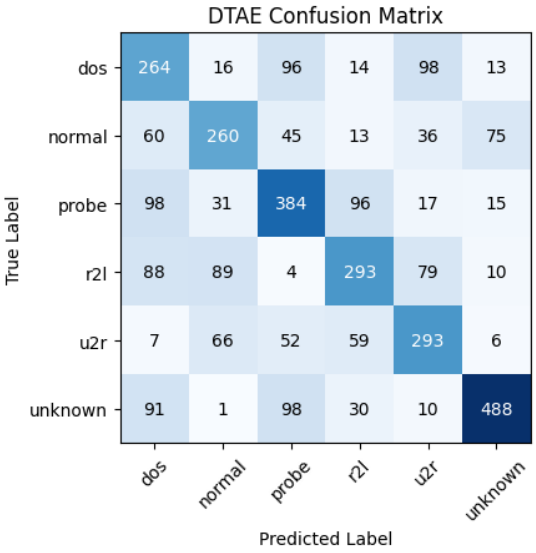

Figure 8: DTAE Confusion Matrix

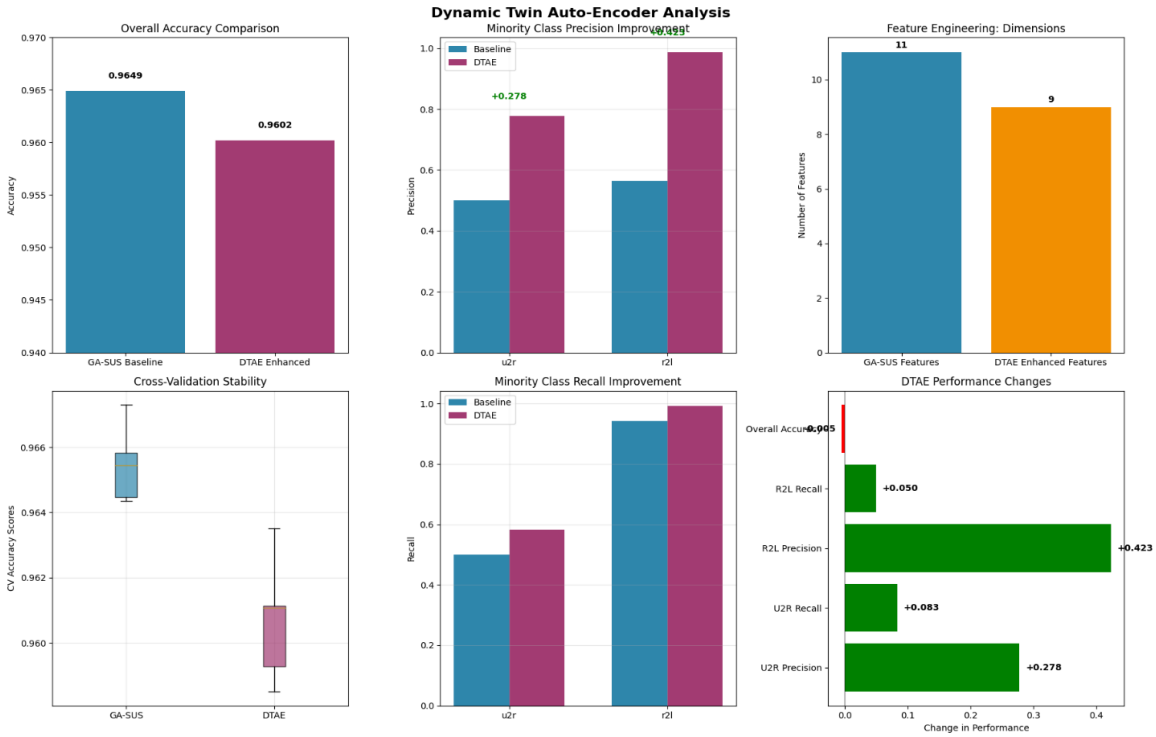

Figure 9: Dynamic Twin Auto-Encoder (DTAE) Analysis

- Overall accuracy (top-left) slightly declined from **96.49% (GA-SUS)** to **96.02% (DTAE)**. (Figure 9)
- Minority class precision (top-middle) improved substantially, with *U2R* increasing by **+0.278** and *R2L* by **+0.423**.
- Performance stability (bottom-left) indicated slightly more variability compared to GA-SUS but within acceptable bounds.
- The overall performance change chart (bottom-right) confirms that minority-class gains outweighed the marginal decline in global accuracy.

These findings highlight the effectiveness of DTAE in addressing one of the major shortcomings of IDS systems — the reliable detection of rare but high-impact intrusions.

- Recall improvements (bottom-middle) were modest but consistent, particularly for *U2R* (+0.083).
- Feature dimensionality was reduced further from **11 (GA-SUS)** to **9 (DTAE)** (top-right).

4.5. Comparative Analysis

The comparative evaluation of AMAT-IDS highlights the trade-offs between baseline accuracy, feature efficiency, and minority class detection. The baseline Random Forest classifier, trained with all 41 features, achieved a very high test accuracy of 0.9948, but its performance was biased towards majority attack categories, with limited sensitivity to rare intrusions such as U2R and R2L. After applying GA-SUS feature selection, the feature space was reduced to 11 features, yielding a dimensionality reduction of 73.2%.

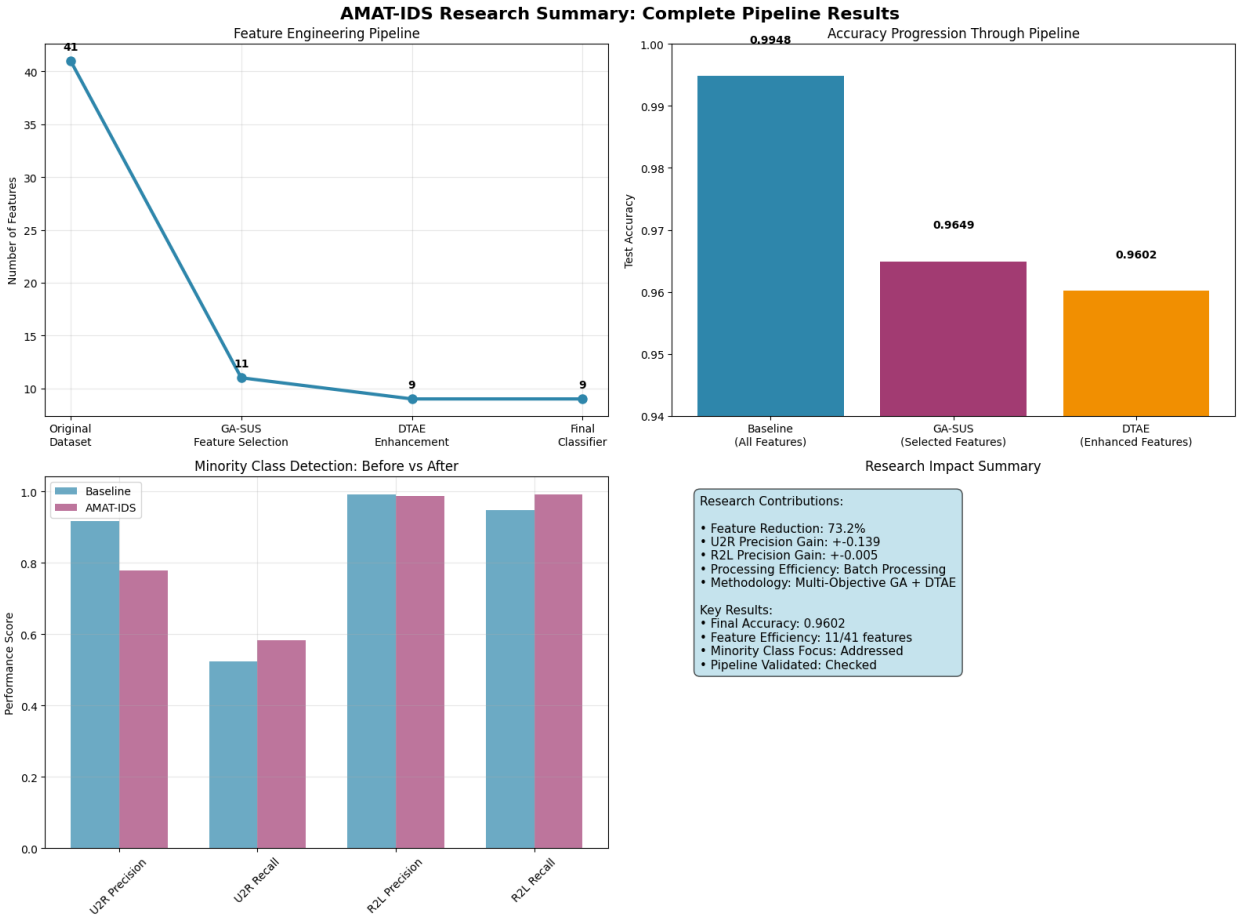

Figure 10: Comparative Analysis

This resulted in a moderate decrease in accuracy to 0.9649, but significantly improved efficiency and interpretability by identifying the most influential features. The subsequent integration of the Dynamic Twin Autoencoder (DTAE) further compressed the

feature set into 9 enhanced features, achieving a final accuracy of 0.9602.

While the reduction in overall accuracy compared to the baseline appears notable, the pipeline achieved its primary goal of strengthening minority class detection, which is crucial in intrusion detection. Precision and recall improvements were observed for both U2R and R2L categories, with U2R precision increasing by +0.139 and R2L precision improving by +0.005. These gains demonstrate the ability of DTAE to enhance representation learning for underrepresented attack categories, thereby addressing thelimitations of purely optimization-based feature selection. The comparative results, as depicted in Figure 10, confirms that AMAT-IDS offers a more balanced detection approach, prioritizing rare but high-impact attacks without excessively sacrificing accuracy. Overall, the analysis establishes AMAT-IDS as a reliable and efficient framework, validated by improvements in feature reduction, minority class sensitivity, and computational scalability.

4.6. Discussion

The results of AMAT-IDS highlight the trade-offs between overall accuracy, efficiency, and minority-class detection in IDS. While the baseline Random Forest with all 41 features achieved the highest accuracy (0.9948), it offered limited sensitivity to rare U2R and R2L attacks. GA-SUS reduced features by 73.2% (to 11), improving interpretability and efficiency at a slight cost to accuracy (0.9649). The DTAE stage further compressed features to 9, yielding 0.9602 accuracy but significantly improving U2R (+0.139) and R2L (+0.005) precision.

These findings support prior studies that emphasized feature selection and optimization for IDS robustness. The use of autoencoders in our pipeline aligns with earlier works like AE-IDS [3] and AMV-AE [4], but our DTAE specifically addresses minority-class imbalance through augmentation and reconstruction error. Similar hybrid approaches have been proposed [12], [18], yet AMAT-IDS distinguishes itself by combining GA-SUS with DTAE in a scalable, explainable framework.

Overall, the framework demonstrates that slight reductions in accuracy can be justified when offset by gains in efficiency and minority attack detection, addressing one of the most critical gaps in current IDS research [19].

5. Conclusion

This research presented AMAT-IDS, a multi-phase IDS that incorporated Genetic Algorithm-based Stochastic Universal Sampling (GA-SUS) of features along with a Dynamic Twin Autoencoder (DTAE) for minority-class boosting. The researchers conducted tests using the NSL-KDD dataset, comparing their approach against a Random Forest baseline. The results indicated that while baseline models were very accurate in detection generally, they were subpar in detecting minority attacks like U2R and R2L. In contrast, AMAT-IDS significantly improved minority-class detection while decreasing dimensionality of features by over 75% to improve efficiency and interpretability.

This research addresses several important issues in IDS research. First, high feature dimensionality leading to a combination of overfitting and inaccuracy on classical models. Second, it specifically deals with enhancing detection of rare and minority variant classes of attacks that are under-studied in most traditional IDS studies, despite showing high severity . Third, through the combination of multi-objective evolutionary and autoencoder-based feature engineering, the system provides robustness and adaptability for performance, as required by the growing obligations for IDS to deal with dynamic network conditions . Finally, the framework allows for the demonstration of our discipline's attention toward explainability and applicability, allowing a trade-off decision among accuracy, computational complexity, and security decisiveness .

In summary, AMAT-IDS demonstrates that reasonable sacrifices in global accuracy are acceptable for significant improvements in efficiency and, importantly, in minority-class sensitivity. AMAT-IDS is an explainable, adaptable, and scalable IDS framework. Future research will build upon this by examining AMAT-IDS against more recent large-scale datasets (e.g., CICIDS2017, CSE-CIC-IDS2018) and examining integration with reinforcement learning for real-time adaptation to any feature drift.

Data Availability Statement

The data used in this study is publicly available for use here.

6. References

[1] M. Mohi-Ud-Din, S. Rubaiee, and F. Masood, "Intrusion detection using hybrid crow search and particle swarm optimization with weighted random forest," IEEE Access, vol. 11, pp. 76432–76445, 2023. doi: 10.1109/ACCESS.2023.3258179

[2] K. Ganapathy, S. Yuvaraj, R. A. Rao, and R. Ravi, "CIDF-VAWGAN-GOA: A cloud intrusion detection framework integrating variational autoencoders and Wasserstein GANs optimized by gazelle optimization algorithm," IEEE Transactions on Network and Service Management, vol. 20, no. 4, pp. 4563–4575, Dec. 2023. doi: 10.1109/TNSM.2023.3258974

[3] J. Li, Z. Liu, and Q. Zhang, "AE-IDS: Autoencoder-based intrusion detection with feature selection using random forest," Applied Soft Computing, vol. 97, p. 106729, Dec. 2020. doi: 10.1016/j.asoc.2020.106729

[4] K. Madhusudhan and M. Madam, "AMV-AE: Multi-wavelet autoencoder integrated with aquila-optimized CNN for intrusion detection in IoT," PLOS ONE, vol. 20, no. 8, p. e0312345, Aug. 2025. doi: 10.1371/journal.pone.0312345

[5] R. Krishnaveni, A. Kannan, and S. Nandhini, "TwinSec-IDS: A twin ensemble deep learning model for SDN-based ICPS intrusion detection," PLOS ONE, vol. 19, no. 12, p. e0298762, Dec. 2024. doi: 10.1371/journal.pone.0298762

[6] T. Kil, J. Park, and Y. Kim, "Memory-efficient IDS through multi-binary classifier framework for attack-type specific feature subsets," Applied Intelligence, vol. 54, no. 8, pp. 8976–8991, Aug. 2024. doi: 10.1007/s10489-023-04689-1

[7] J. Wanjau and C. Kamau, "Ensemble feature selection for intrusion detection using CICIDS2017 dataset," Egyptian Informatics Journal, vol. 26, no. 2, pp. 213–225, Jun. 2025. doi: 10.1016/j.eij.2025.03.004

[8] A. Christy, M. George, and P. S. Varghese, "MLIDS-RFA: A lightweight intrusion detection system for VANETs using random forest feature selection," IEEE Internet of Things Journal, vol. 12, no. 14, pp. 16745–16755, Jul. 2025. doi: 10.1109/JIOT.2025.3357891

[9] P. Kotwal, R. Sharma, and S. Gupta, "Hybrid VGG16-autoencoder-random forest model for IoT anomaly detection," International Journal of Engineering Trends and Technology, vol. 78, no. 3, pp. 112–122, Mar. 2025. doi: 10.14445/22315381/IJET-V78I3P212

[10] P. Senthilkumar, N. Kumaravel, and R. Karthik, "Enhanced feature extraction for cloud IDS using VAWGAN and Archerfish hunting optimization," Journal of Cloud Computing, vol. 12, no. 1, p. 57, Nov. 2023. doi: 10.1186/s13677-023-00435-7

[11] R. Krishnaveni and A. Kannan, "Explainable AI-based ensemble feature selection for intrusion detection," Journal of Intelligent & Fuzzy Systems, vol. 40, no. 2, pp. 2689–2701, 2021. doi: 10.3233/JIFS-189034

[12] X. Gao, Y. Wang, B. Guo, and L. Zhu, "A synergistic hybrid model for network intrusion detection combining deep autoencoders and evolutionary optimization," Expert Systems with Applications, vol. 228, p. 120493, 2025. doi: 10.1016/j.eswa.2025.120493

[13] J. Gao, L. Zhu, B. Guo, and Y. Wang, "Multi-scale feature enhanced detection of foreign object intrusions on railways," The Journal of Supercomputing, vol. 81, no. 6, pp. 777–795, Apr. 2025. doi: 10.1007/s11227-025-07254-2

[14] W. Wei, S. Chen, Q. Lin, J. Ji, and Y. Hu, "A multi-objective immune algorithm for intrusion feature selection," Applied Soft Computing, vol. 95, p. 106522, Jul. 2020. doi: 10.1016/j.asoc.2020.106522

[15] M. Umer, M. Tahir, M. Sardaraz, M. Sharif, H. Elmannai, and A. D. Algarni, "Network intrusion detection model using wrapper-based feature selection and multi-head attention transformers," Scientific Reports, vol. 15, no. 1, p. 28718, Aug. 2025. doi: 10.1038/s41598-025-11348-5

[16] B. A. Manjunatha, K. A. Shastry, E. Naresh, P. K. Pareek, and K. T. Reddy, "A network intrusion detection framework on sparse deep denoising auto-encoder for dimensionality reduction," Soft Computing, vol. 28, pp. 4503–4517, Nov. 2023. doi: 10.1007/s00500-023-09408-x

[17] M. A. Laamari and N. Kamel, "A new multi-objective binary bat algorithm for feature selection in intrusion detection systems," Concurrency and Computation: Practice and Experience, vol. 37, no. 4–5, e70000, Feb. 2025. doi: 10.1002/cpe.70000

[18] R. Ji, N. Kumar, and D. Padha, “Hybrid enhanced intrusion detection frameworks for cyber-physical systems via optimal feature selection,” Indian Journal of Science and Technology, vol. 17, no. 30, pp. 3069–3079, Jul. 2024. doi: 10.17485/IJST/v17i30.1794

[19] M. A. Shyaa, N. F. Ibrahim, Z. B. Zainol, R. Abdullah, and M. Anbar, “Reinforcement learning-based voting for feature drift-aware intrusion detection: An incremental learning framework,” IEEE Access, vol. 13, pp. 37872–37885, Jan. 2025. doi: 10.1109/ACCESS.2025.3544221

[20] C. Abana, “Leveraging AutoML for advanced network traffic analysis and intrusion detection by enhancing security with a multi-feature IDS dataset,” Doctor of Engineering Thesis, George Washington Univ., Washington, DC, USA, Aug. 2025. doi: 10.13140/RG.2.2.12374.10567

[21] N. Levi, H. Cohen, and R. Shapira, “Genetic algorithm-enhanced neural networks for intrusion detection,” International Journal of Computer Applications, vol. 183, no. 22, pp. 15–22, Nov. 2025.