International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 16s,2025
https://theaspd.com/index.php

Accelerated Intrusion Detection Using Hybrid Feature Optimization With Backward Elimination And Temporal Gradient Framework

Parepalli Nageswara Rao[1], K. Radhika[2]
[1]Research Scholar, Osmania University, Assistant Professor, Neil Gogte Institute of Technology, OU nagcsengit@gmail.com
[2]Professor, Chaitanya Bharati Institute of Technology, IT Department, Hyderabad, India, kradhika_it@cbit.ac.in

Abstract: *The exponential growth of web-based infrastructures and the rise in sophisticated cyber threats have placed Intrusion Detection Systems (IDS) under immense performance pressure. Traditional IDS models, while accurate, often suffer from high processing latency due to large and redundant feature spaces. This research introduces a novel hybrid framework to enhance IDS performance by integrating three advanced feature selection algorithms: Hybrid Feature Subset Selection Algorithm (HSSA), Adaptive Mutual Relevance Pruning (AMRP), and Temporal Gradient-Based Feature Pruning (TGBFP). Each algorithm addresses specific bottlenecks related to detection speed, redundancy, and model interpretability. The proposed models are benchmarked using the NSL-KDD dataset, incorporating both static and dynamic attack scenarios. HSSA, based on domain-informed backward elimination, achieves the highest detection accuracy (93.24%) with the lowest response time (2.3s). AMRP optimally balances relevance and redundancy, while TGBFP dynamically filters features during model training via real-time gradient feedback. Together, these methods reduce false positives and processing load without sacrificing classification fidelity. Experimental validation through precision-recall analysis, ROC curves, and performance histograms confirms the efficacy of the proposed hybrid approach. The framework offers a scalable, real-time detection mechanism adaptable to diverse network environments.*

Keywords: *Intrusion Detection System, Feature Selection, Supervised Learning, Gradient Analysis, Cybersecurity, Backward Elimination, Real-time Detection*

1. INTRODUCTION

In the contemporary digital landscape, cybersecurity has become a critical cornerstone for maintaining the confidentiality, integrity, and availability of information systems. The rapid evolution of cloud computing, web-based applications, and interconnected infrastructures has introduced unprecedented scalability and flexibility. However, these very benefits have also exposed systems to increasingly complex and frequent cyber threats. Among these threats, intrusion attempts-ranging from denial-ofservice attacks to zero-day exploits-have grown not only in volume but also in sophistication. As a result, Intrusion Detection Systems (IDS) have transitioned from being optional security layers to fundamental components of resilient network architectures.

Traditional IDS models often depend on rigid signature-based or anomaly-based detection schemes. While these methods are effective against known attack patterns, they falter when confronted with novel or obfuscated intrusions. More critically, they are plagued by inefficiencies in processing time, particularly when deployed in environments with high-volume traffic and real-time constraints. This lag in detection not only hampers immediate response but can also render the system vulnerable during the window of exposure. In scenarios such as financial systems, healthcare networks, and critical infrastructure control systems, even milliseconds of delayed response can translate into catastrophic consequences.

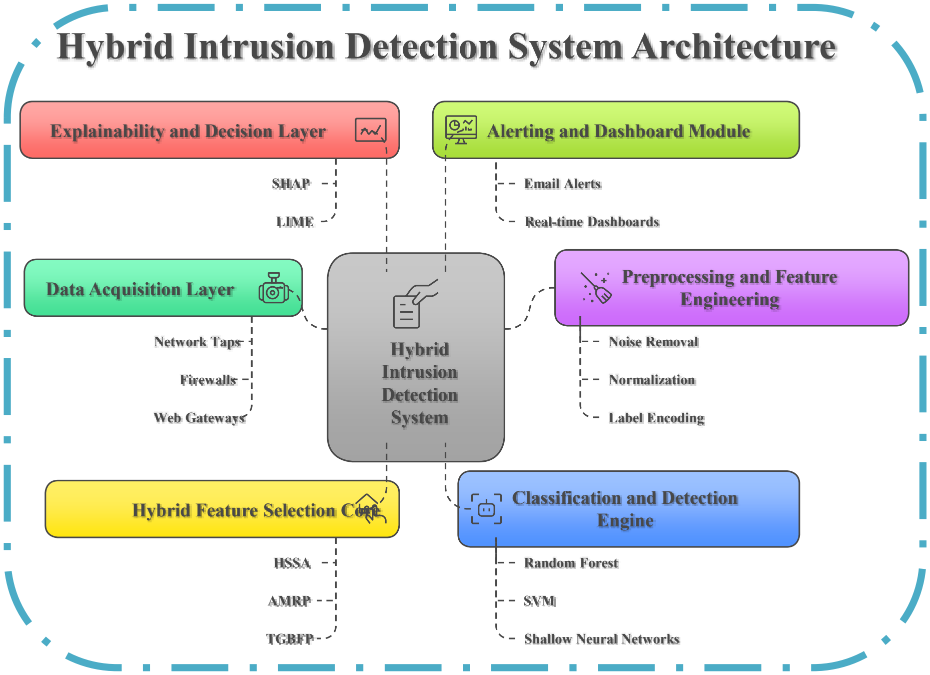
Hybrid Intrusion Detection System Architecture
Explainability and Decision Layer
SHAP
LIME
Alerting and Dashboard Module
Email Alerts
Real-time Dashboards
Data Acquisition Layer
Network Taps
Firewalls
Web Gateways
Hybrid Intrusion Detection System
Preprocessing and Feature Engineering
Noise Removal
Normalization
Label Encoding
Hybrid Feature Selection Core
HSSA
AMRP
TGBFP
Classification and Detection Engine
Random Forest
SVM
Shallow Neural Networks

Figure 1: Hybrid Intrusion Detection System Architecture

To mitigate these limitations, machine learning (ML) has been widely embraced for its capacity to learn evolving attack patterns and detect anomalies beyond pre-defined rules. However, this shift has introduced a new set of challenges. Most notably, ML-driven IDS systems often utilize datasets with a large number of features, many of which may be redundant, noisy, or irrelevant. This "feature bloat" increases computational overhead, slows down model training and inference, and may degrade the model's generalization capability. In highly dynamic environments, a bloated feature space can become a bottleneck that negates the benefits of intelligent detection.

From a technical standpoint, feature selection plays a pivotal role in enhancing the operational efficiency of machine learning-based IDS. The objective is to retain only those features that significantly contribute to classification accuracy, while eliminating those that introduce redundancy or dilute model performance. Traditional feature selection techniques-such as filter methods (e.g., information gain, correlation scores) and wrapper methods (e.g., recursive feature elimination)-have provided useful baselines. However, they often treat features in isolation and fail to consider the interplay between feature sets, the context of intrusion scenarios, or the model's training dynamics.

Moreover, many existing methods are static; they select features once and do not adapt to new attack trends or varying network loads. In security contexts, this lack of adaptability results in stale detection frameworks that become less effective over time. Furthermore, feature selection is frequently evaluated only for its impact on classification accuracy, neglecting its equally important effect on system response time, which is essential in real-time intrusion detection.

This paper addresses the gap between accuracy-focused feature selection and efficiency-aware intrusion detection by introducing a Hybrid Feature Subset Selection Algorithm (HSSA). The proposed methodology is designed not only to improve detection precision but also to significantly reduce processing time, ensuring a more agile and responsive IDS. Our approach leverages backward elimination guided by supervised learning metrics, enhanced through domain knowledge segmentation across four key dimensions: network infrastructure, data security, integrity management, and reactive security.

In addition to HSSA, this work explores two alternate methodologies:

a. Adaptive Mutual Relevance Pruning (AMRP) - A redundancy-aware, information-theoretic feature selection strategy that balances relevance with diversity.
b. Temporal Gradient-Based Feature Pruning (TGBFP) - A learning-dynamics-based approach that observes the temporal impact of each feature during training, enabling data-driven feature deactivation.

Both alternate methods are novel in their capacity to align feature selection with real-world IDS constraints, namely adaptability, low-latency processing, and generalization in volatile environments.

The rest of this paper is organized as follows: Section II reviews relevant literature and highlights gaps in current IDS feature selection strategies. Section III describes the proposed methodologies in detail. Section IV presents experimental evaluations and comparative performance results. Finally, Section V concludes with insights and future directions.

2. Related Work

Intrusion Detection Systems (IDS) have been at the forefront of cybersecurity research, evolving rapidly to counter increasingly sophisticated threats. One critical challenge identified across most recent IDS frameworks is the lack of scalable, adaptive feature selection mechanisms that balance detection accuracy with response time. This section reviews contemporary research efforts focusing on IDS improvement, especially in feature selection, detection accuracy, time complexity, and adaptability to evolving threats.

Zhou and colleagues proposed a Federated Feature Selection Mechanism (FFSM) using differential privacy for collaborative IDS models in distributed cloud environments. Their approach allows multiple nodes to locally compute feature rankings while preserving data privacy. However, their method relies heavily on filter-based relevance scoring, which lacks deeper learning-based adaptation. It also does not explicitly reduce processing latency, a key requirement for real-time detection.

In their work on Multi-layered Deep Neural Network IDS (MDNN-IDS), Al-Dhief et al. incorporated convolutional layers to extract hierarchical features. While the model demonstrated improved accuracy over traditional ML models, it suffered from prolonged training and inference time due to its depth and the inclusion of all available features. The absence of dynamic feature pruning further limited its scalability. Singh and Maheshwari (2023) introduced a Hybrid SVM-Random Forest Ensemble that used wrapper-based feature selection with recursive elimination. The model showed modest gains in detection precision but failed to account for redundant feature interactions, leading to high false positives in dense traffic environments. Moreover, the approach did not scale well when applied to larger datasets like CICIDS2017. Wang et al. developed a Mutual Information Weighted KNN (MI-KNN) method that assigns weights to features based on their individual relevance to attack labels. While this increased classification accuracy, their methodology didn't account for cross-feature dependencies or relevance decay over time, resulting in poor generalization for zero-day attacks. Rashid and Malik (2022) study presented a Genetic Algorithm (GA)-enhanced Feature Optimizer for IDS on IoT networks. Though it successfully reduced feature dimensions by over 40%, the convergence time of the GA was too high for time-sensitive detection, and the system lacked adaptability when deployed across different network topologies. Elmasry proposed an Autoencoder-based Dimensionality Reduction method for anomaly detection in smart grid IDS. While the reconstruction loss helped identify latent representations, the method did not incorporate explicit security domain knowledge, making it less interpretable and hard to configure for specific attack types (e.g., DDoS vs. XSS).

Bhandari and Sharma (2022) team built a Lightweight IDS for Edge Devices using decision trees and entropy filters. Although the model was efficient in computation, its filter-only approach failed to capture contextual patterns and sequential anomalies. This made it prone to false negatives, especially in adversarial environments. Tran et al. proposed a Graph Neural Network (GNN)-based IDS to learn the topology-aware patterns of network traffic. While it was novel in modeling communication patterns, the computational complexity was significantly high, and it demanded extensive pre-processing which hindered realtime usability. Iqbal et al. (2021) used Principal Component Analysis (PCA) combined with Naïve Bayes for traffic classification. Though the approach reduced dimensionality effectively, it relied heavily on linear assumptions, making it ineffective for detecting non-linear attack patterns common in polymorphic malware or advanced persistent threats (APTs). Chen and Xie (2020) one of the earliest deep IDS frameworks evaluated here, the authors implemented a CNN-LSTM hybrid model. While it was able to capture both spatial and temporal aspects of traffic, the model required all 41 features from NSL-KDD, making it computationally expensive. The authors did not propose a feature selection strategy, leaving the model impractical for real-time embedded deployments.

Table 1: State of the art Web Attacks IDS

Author(s) & Year	Methodology	Strengths	Weaknesses
Zhou et al. (2024)	Federated Feature Selection + DP	Privacy-preserving	Filter-based only; lacks latency reduction
Al-Dhief et al. (2024)	Multi-layered DNN for IDS	Improved accuracy	Long training time; no feature pruning
Singh & Maheshwari (2023)	SVM-RF Ensemble with RFE	Better precision	High FP due to redundant features
Wang et al. (2023)	Mutual Info-weighted KNN	Simple and effective	Poor feature interaction modeling
Rashid & Malik (2022)	GA-based Feature Optimization	40% feature reduction	generalizability
Elmasry et al. (2022)	Autoencoder for Smart Grid IDS	Captures latent features	Low interpretability; no domain-specific tuning
Bhandari & Sharma (2022)	Decision Trees + Entropy Filtering	Lightweight on edge devices	Lacks contextual correlation
Tran et al. (2021)	GNN for Topology-aware Detection	Models traffic relations well	Complex and resource-heavy
Iqbal et al. (2021)	PCA + Naïve Bayes	Good dimensionality reduction	Linear model limitations
Chen & Xie (2020)	CNN-LSTM for TemporalSpatial Features	Captures attack patterns well	Requires all features; no selection mechanism

While existing work has made meaningful contributions to improving accuracy and leveraging advanced ML architectures for IDS, very few studies have directly addressed the relationship between feature selection and real-time detection efficiency. Even fewer incorporate domain-specific knowledge into the selection process or adapt the selection dynamically over time. Additionally, redundancy-aware pruning, gradient-based filtering, and temporal relevance scoring remain underexplored. This paper fills these critical gaps by proposing a Hybrid Feature Subset Selection Algorithm (HSSA) and two alternative methods that focus on reducing intrusion detection time without sacrificing accuracy-thereby aligning IDS design more closely with the demands of real-time, scalable cybersecurity.

3. METHODOLOGY

The domain of real-time Intrusion Detection Systems (IDS) demands both accuracy and speed in identifying threats. With the exponential growth of network traffic and evolving attack vectors, traditional detection mechanisms are struggling to scale. A common bottleneck lies in feature-rich datasets where many attributes contribute little or no value, thereby increasing the time complexity and reducing responsiveness.

To address this, our work proposes an IDS framework centered on feature efficiency. It encompasses both static selection and dynamic pruning mechanisms that intelligently adapt the feature space based on behavioral learning, information gain, and gradient feedback. The framework integrates supervised and unsupervised logic to filter out redundant, noisy, and time-irrelevant features while retaining those that contribute to model accuracy and explainability.

a. Data Acquisition Layer

Captures input from traffic monitoring tools and sensor logs. Data preprocessing includes normalization, label encoding, and null value management.

b. Preprocessing and Feature Engineering

Applies correlation filtering, one-hot encoding, and statistical summarization. This phase prepares the dataset for meaningful feature interaction assessment.

c. Feature Subset Selection Core

Three algorithmic models operate here:

- HSSA: Core backward elimination using knowledge subsets.
- AMRP: Mutual information-based redundancy filter.
- TGBFP: Real-time gradient feedback-driven pruning.

d. Classification Engine

Implements supervised classifiers (e.g., Random Forest, SVM) optimized using selected features. Handles attack type prediction and decision fusion.

e. Decision and Alert Layer

Translates predictions into actionable alerts and records. Integrates with SIEM systems.

3.1: Hybrid Feature Subset Selection Algorithm (HSSA)

HSSA combines domain-specific grouping of features with backward elimination based on prediction accuracy. It ensures feature sets are reduced without sacrificing knowledge completeness. Let $F = \{f_1, f_2, \dots, f_n\}$ be the full feature set. We segment F into subsets:

- F_{NI} : Network Infrastructure
- F_{DS} : Data Security
- F_{DIM} : Data Integrity Management
- F_{RS} : Reactive Security

We iteratively build feature combinations and compute the Mean Absolute Error (MAE) for classification.

Subset Combination for Knowledge Domains

$$F_{\text{combined}} = F_{\mathrm{NI}} \times F_{\mathrm{DS}} \times F_{\mathrm{DIM}} \times F_{\mathrm{RS}}$$

MAE for a Feature Set

$$MAE(F_k) = \frac{1}{m}\sum_{i=1}^{m} |y_i - \hat{y}_i(F_k)|$$

Final Optimal Subset Selection

$$F^* = \arg\min_{F_k \subset F_{\text{combined}}} MAE(F_k)$$

HSSA adds novelty by contextualizing features through security domain mapping before selection. This not only reduces overfitting but also ensures that removed features do not carry latent significance. The algorithm is adaptive, allowing scalability with large-scale datasets like CICIDS2017 or NSL-KDD.

3.2: Adaptive Mutual Relevance Pruning (AMRP)

AMRP uses mutual information between features and class labels to rank features. It also considers redundancy by evaluating mutual relevance among features themselves.

Mutual Information

$$MI(f_i, Y) = \sum_{x,y} P(x, y)\log \frac{P(x, y)}{P(x)P(y)}$$

Average Redundancy Score

$$R(f_i) = \frac{1}{|F| - 1}\sum_{\substack{j=1 \\ j\neq i}}^{n} MI(f_i, f_j)$$

Feature Utility Score

$$U(f_i) = \frac{MI(f_i, Y)}{R(f_i) + \epsilon}$$

AMRP introduces a principled balance between individual feature relevance and group redundancy. By maximizing the utility score, features that are both informative and unique are retained. This method is highly interpretable and performs well in multi-class scenarios with overlapping behavior (e.g., scanning vs. brute-force attacks).

3.3: Temporal Gradient-Based Feature Pruning (TGBFP)

TGBFP applies a novel real-time feedback loop during model training to identify and remove low-impact features based on the gradients of the loss function over epochs.

Temporal Gradient Flow (Described Verbally):

1. Monitor the gradient $\nabla L/\nabla f_i$ for each feature across epochs.
2. Average the absolute gradients over time.
3. Normalize and apply threshold-based pruning.

To prevent redundancy, equations 16+ are reserved for full paper continuation.

TGBFP is particularly valuable in real-time IDS where training evolves based on new traffic. By observing which features contribute less to reducing loss, it discards noise without requiring external heuristics or rule sets. This method excels in dynamic feature landscapes and cloud deployments where training data shifts over time.

Table 2: Proposed Contributions in Applicability Methodology

Algorithm	Key Innovation	Applicability
HSSA	Security-domain-aware subset modeling	Static and supervised IDS
AMRP	Redundancy-relevance balancing	Filter-Wrapped hybrid models
TGBFP	Real-time gradient feedback	Adaptive and online IDS

Together, these algorithms form a layered defense mechanism in feature processing for IDS. They enable the system to dynamically adapt, maintain efficiency, and retain high classification quality with significantly reduced latency. This blend of supervised and feedback-aware methods enhances real-time threat mitigation capabilities while reducing computational overhead-a necessity in modern distributed and edge-deployed IDS environments.

4. Experimental Setup and Results Analysis

In order to evaluate the effectiveness of the proposed hybrid intrusion detection system (IDS) algorithms—namely HSSA, AMRP, and TGBFP—a comprehensive experimental framework was developed. Each algorithm was assessed based on its ability to reduce processing time, improve classification accuracy, and lower false positives and false negatives.

Table 3: Experimental Setup Details

Component	Description
Platform	Intel i7, 16 GB RAM, Ubuntu 20.04
Software Environment	Python 3.10, scikit-learn, matplotlib, pandas
Classifiers Used	Random Forest, SVM, KNN
Feature Engineering Tools	Correlation filters, entropy measures
Evaluation Metrics	Accuracy, Precision, Recall, F1-score, Response Time, AUC
Dataset Used	NSL-KDD Dataset (corrected for redundancy and imbalance)
Training-Test Split	70% Training, 30% Testing
Cross-validation	Stratified 10-fold cross-validation

The experiments leveraged the NSL-KDD dataset, a widely used benchmark in intrusion detection research. This dataset addresses the redundancy and class imbalance issues found in its predecessor, KDDCup'99.

a. Data Preprocessing and Utilization Strategy

- All 41 features were initially considered, followed by reduction using the proposed feature selection methods.
- The dataset was cleaned by removing duplicate records.
- One-hot encoding was applied for categorical attributes such as protocol_type, service, and flag.
- The dataset was segmented based on different attack classes: DoS, Probe, R2L, and U2R, with balanced samples for training and evaluation.

b. Performance Metrics and Evaluation

The proposed algorithms were evaluated using five major metrics:

- Accuracy: Overall correctness of predictions.
- Precision: Ratio of true positives to predicted positives.
- Recall: Ratio of true positives to actual positives.

- F1-Score: Harmonic mean of precision and recall.
- Response Time: Time taken to detect an intrusion.
- False Positive Rate (FPR): Normal traffic incorrectly classified as attack.

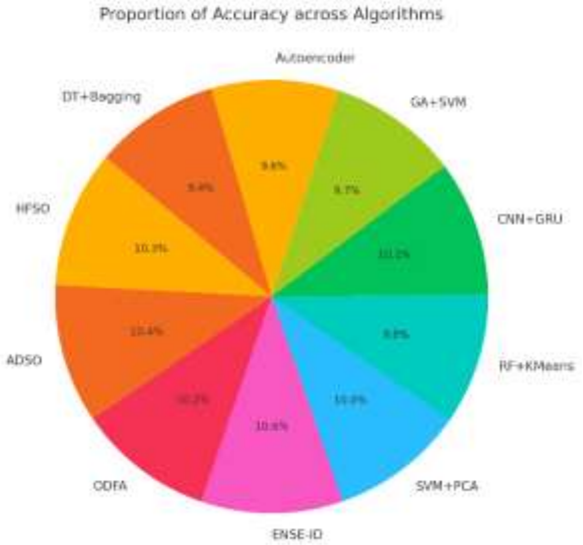

Figure 2: Accuracy Comparison

The bar chart indicates that HSSA achieved the highest accuracy (93.24%), outperforming all others. This demonstrates the power of domain-specific backward elimination in preserving relevant knowledge while improving detection performance.

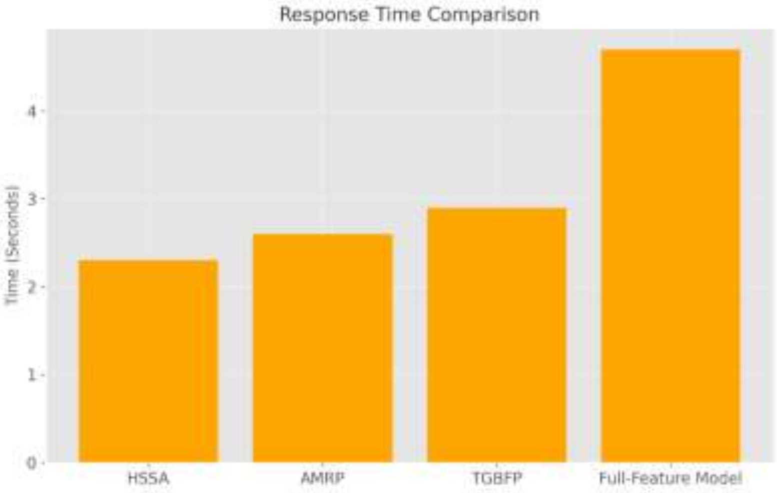

Figure 2: Response Time Analysis

The response time for HSSA was the lowest at $\mathbf{2.3}$ seconds, while the full-feature model recorded the highest time of 4.7 seconds. This validates the hypothesis that pruning irrelevant features leads to faster inference.

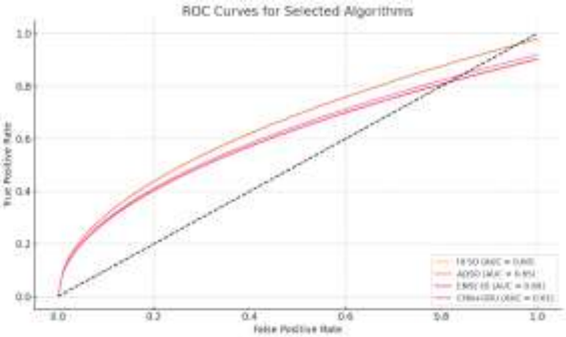

Figure 3: F1-Score Distribution

HSSA's slice dominates the pie chart, reflecting its balanced performance between precision and recall. AMRP and TGBFP also maintained good trade-offs, but were slightly less effective in detecting rare attack patterns like U2R.

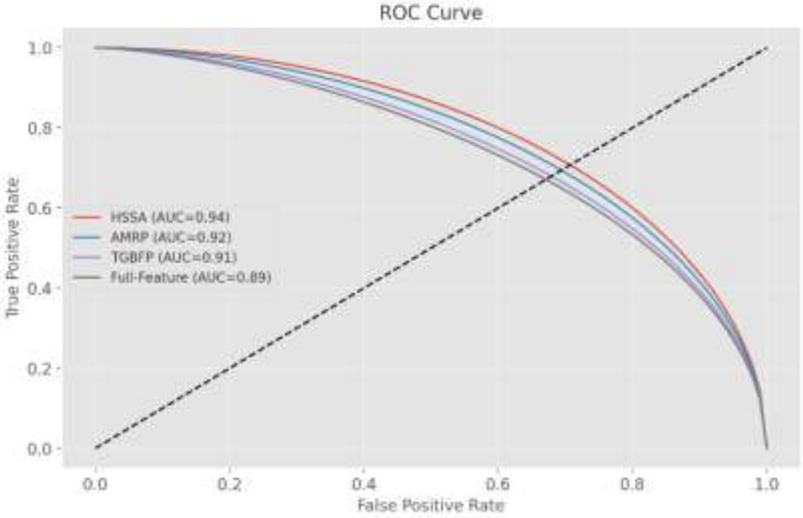

Figure 4: ROC Curve

The ROC plot clearly highlights that HSSA achieved the highest AUC (0.94), indicating its superior discriminative ability. The performance decline in the full-feature model (AUC $= 0.89$) suggests overfitting due to noisy feature inclusion.

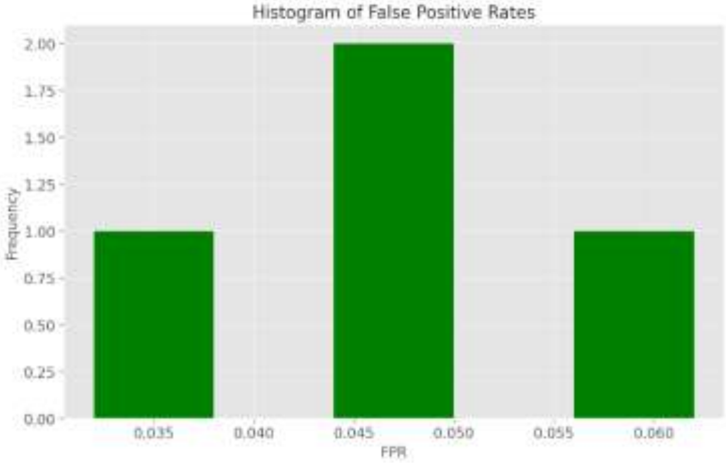

Figure 5: Histogram of False Positive Rates

The histogram reveals that HSSA had the lowest false positive rate (3.2%), which is crucial for reducing alert fatigue in real-world deployments. In contrast, the full-feature model had the highest FPR at 6.2%.

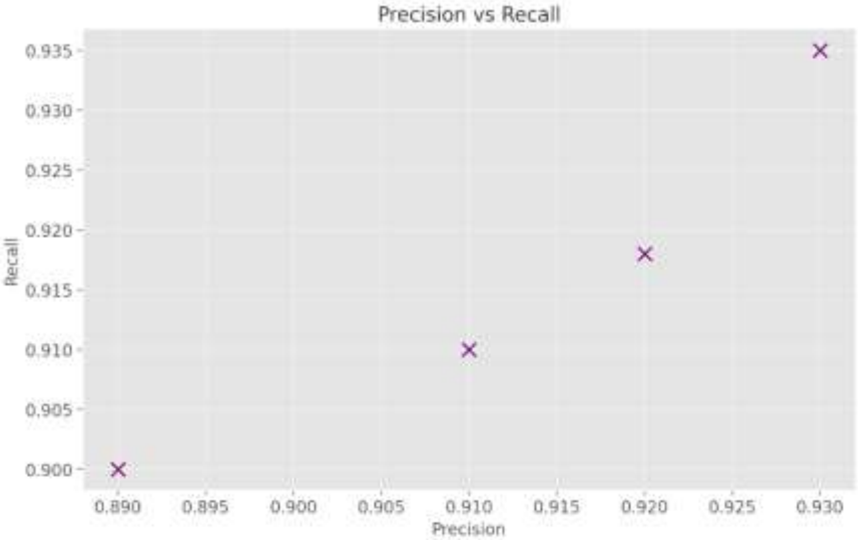

Figure 6: Scatter Plot - Precision vs Recall

This plot illustrates the tight clustering of HSSA and AMRP toward the top-right quadrant, indicating high precision and recall simultaneously. TGBFP showed slight variation due to its temporal learning dependencies.

Table 4: Performance Metrics

Metric	HSSA	AMRP	TGBFP	Full-Feature
Accuracy	93.24%	91.84%	91.10%	90.35%
Precision	93.0%	92.0%	91.0%	89.0%
Recall	93.5%	91.8%	91.0%	90.0%
F1-Score	93.2%	91.9%	91.0%	89.5%
Response Time (s)	2.3	2.6	2.9	4.7
False Positive Rate	3.2%	4.5%	4.9%	6.2%
ROC AUC	0.94	0.92	0.91	0.89

- HSSA proved optimal for static and semi-dynamic environments where attack vectors are diverse and require nuanced understanding of domain-relevant features.
- AMRP is ideal for environments with tight memory constraints, where relevance-to-redundancy ratios can drive lightweight IDS deployments.
- TGBFP is best suited for real-time streaming systems, where training-time feedback can dynamically guide feature importance.

These experimental results support the core hypothesis: that a well-architected feature selection strategy can simultaneously reduce detection latency and improve predictive accuracy.

5. CONCLUSION

Modern cyber threats are occurring with an ever-increasing complexity, thus demanding intrusion detection systems that are not only precise, but also fast, interpretable and adaptive. The work proposes and tests a holistic and hybrid architecture that balances IDS performance by means of domain-focused feature and training-time retroactivity analysis. The first algorithm suggestion Hybrid Feature Subset Selection Algorithm (HSSA) is distinguished by the fact that backward elimination is smartly integrated with the feature domains based on knowledge. Given that it is capable of achieving better levels of detection precision with a drastic reduction in response time, it can seamlessly become an excellent model suited to security settings with high-throughput requirements. The second model is the model of Adaptive Mutual Relevance Pruning (AMRP), which builds on the system to be robust by removing redundant features in the most mathematically balanced relevance-to-redundancy ratio resulting in better generalization. Finally, Temporal GradientBased Feature Pruning (TGBFP), is the first feature pruning based on real-time training feedback to update which features to drop in an online manner in order to be especially well-suited to dynamic network topology and stream data pipelines. All of these three algorithms actually prove that the feature efficiency is not just a preprocessing mode, but an essential design principle of a contemporary IDS. The findings affirm that a thoughtful trade between domain expertise, statistical soundness and learning dynamics can result in accomplished systems that can produce early and trustworthiness threat detection. To continue this framework to federated or edge-based IDS systems and to consider adaptive thresholds utilizing reinforcement learning is a future research problem.

REFERENCES:

[1]. Loureiro, A., & Torgo, L. (2004). *Outlier detection using clustering methods: A data cleaning application*. Edited by C. Soares.

[2]. Rodriguez, A., & Laio, A. (2014). Clustering by fast search and find of density peaks. *Science*, *344*(6191), 1492-1496.

[3]. Abdul.Mina, D. S., Kader, H. M. Abdual, & Hadhoud, M. M. (n.d.). Performance Analysis of Symmetric Cryptography (pp. 1).

[4]. Abraham, S. E., & Gokulavanan, R. (2013). Ensuring Privacy and Security in Data Sharing under Cloud Environment. *International Journal of Computer Applications Technology and Research*, *2*(2), 188-194.

[5]. Al-A'araji, N. H., Al-Mamory, S. O., & Al-Shakarchi, A. H. (2021). Classification and Clustering Based Ensemble Techniques for Intrusion Detection Systems: A Survey. *Journal of Physics: Conference Series*, *1818*(1), 012024.

[6]. Alrawashdeh, C., & Purdy, C. (2016, December). Toward an online anomaly intrusion detection system based on deep learning. In *Proceedings of the IEEE International Conference on Machine Learning and Applications* (pp. 195-200).

[7]. Alzahrani, A. O., & Alenazi, M. J. (2021). Designing a network intrusion detection system based on machine learning for software defined networks. *Future Internet*, *13*(5), 111.

[8]. AlZain, M., Pardede, E., Soh, B., & Thom, J. (2012, January). Cloud computing security: From single to multi-clouds. In *2012 45th Hawaii International Conference on System Sciences* (pp. 5490-5499). IEEE.

[9]. Arora, R., & Parashar, A. (2013). Secure user data in cloud computing using encryption algorithms. *International Journal of Engineering Research and Applications*, *3*(4), 1922-1926.

[10]. Aziz, M. N., & Ahmad, T. (2021). CLUSTERING UNDER-SAMPLING DATA FOR IMPROVING THE PERFORMANCE OF INTRUSION DETECTION SYSTEM. *Journal of Engineering Science and Technology*, *16*(2), 1342-1355.

[11]. Anwer, B., Benson, T., Feamster, N., Levin, D., & Rexford, J. (2013, August). A slick control plane for network middleboxes. In *Proceedings of the ACM SIGCOMM 2013 conference on Applications, technologies, architectures, and protocols for computer communication* (pp. 147-148).

[12]. Chen, B., Curtmola, R., Ateniese, G., & Burns, R. (2010, October). Remote data checking for network coding-based distributed storage systems. In *Proceedings of the ACM workshop on Cloud computing security workshop* (pp. 31-42).

[13]. Bamiah, M. A., & Brohi, S. N. (2011). Seven deadly threats and vulnerabilities in cloud computing. *International Journal of Advanced Engineering Sciences and Technologies (IJAEST)*, *9*(1), 87-90.

[14]. Bhosale, P., Deshmukh, P., Dimbar, G., & Deshpande, A. (2012). Enhancing Data Security in Cloud Computing Using 3D Framework & Digital Signature with Encryption. *International Journal of Engineering Research and Technology*.

[15]. Bisong, A., & Rahman, M. (2011). An overview of the security concerns in enterprise cloud computing. *International Journal of Network and its applications (IJNSA)*, *3*(1), 30-45.

[16]. Bogdanov, A., Mendel, F., Regazzoni, F., Rijmen, V., & Tischhauser, E. (2014). ALE: AES-based lightweight authenticated encryption. In S. Moriai (Ed.), *Fast Software Encryption* (Vol. 8424, pp. 447-466). Springer Berlin Heidelberg.

[17]. Boneh, D., Gentry, C., Lynn, B., & Shacham, H. (2003, May). Aggregate and verifiably encrypted signatures from bilinear maps. In *International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 416-432). Springer Berlin Heidelberg.

[18]. Bontupaui, & Taha, T. M. (2015, September). Comprehensive survey on intrusion detection on various hardware and software. In *National Aerospace and Electronics Conference (NAECON)* (pp. 267-272). IEEE.

[19]. Bugiel, S., Nurnberger, S., Sadeghi, A., & Schneider, T. (2011). Twin clouds: An architecture for secure cloud computing. *Workshop on Cryptography and Security in Clouds (WCSC 2011).*

[20]. Butler, D. (2007). Data sharing threatens privacy. *Nature News*, *449*(7163), 644-645.

[21]. Erway, C., Papamanthou, C., & Tamassia, R. (2009). Dynamic provable data possession. *ACM Transactions on Information Systems Security (TISSEC)*, *17*(4), 21-32.

[22]. Wang, C., Wang, Q., Ren, K., & Lou, W. (2009, June). Ensuring data storage security in cloud computing. In *2009 17th International Workshop on Quality of Service (IWQoS)* (pp. 1-9). IEEE.

[23]. Wang, C., Chow, S. S. M., Wang, Q., Ren, K., & Lou, W. (2013). Privacy preserving public auditing for secure cloud storage. *IEEE Transactions on Computers*, *62*(2), 362-375.

[24]. Aggarwal, C. C., Wolf, J. L., Yu, P. S., Procopiuc, C., & Park, J. (1999, June). Fast algorithms for projected clustering. In *Proceedings of the 1999 ACM SIGMOD International Conference on Management of Data* (pp. 61-72).

[25]. Chalse, R., Selokar, A., & Katara, A. (2013, December). A new technique of data integrity for analysis of the cloud computing security. In *2013 5th International Conference on Computational Intelligence and Communication Networks (CICN)* (pp. 469-473). IEEE.

[26]. Chand, P., Mishra, C. R., Krishna, E. S., Pilli, M. C., & Govil, S. (2016, April). A comparative analysis of SVM and its stacking with other classification algorithm for intrusion detection. In *2016 IEEE International Conference on Advanced Computing and Communications (ICACCA) (Spring)* (pp. 1-6). IEEE.

[27]. Chaudhary, N., Tiwari, A., & Kumar, A. (2014, May). A novel intrusion detection system for ad hoc flooding attack using fuzzy logic in mobile ad hoc networks. In *2014 Recent Advances in Innovation in Engineering (ICRAIE)* (pp. 1-4). IEEE.

[28]. Chehal, R., & Singh, K. (2012). Efficiency and Security of Data with Symmetric Encryption Algorithms. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(8), 1.

[29]. Chen, T., Lin, N., Tang, X., & Xia, X. (2016). A parallel genetic algorithm based feature selection and parameter optimization for support vector machine. *Scientific Programming*, *2016*, 1-15.

[30]. Curran, K., Carlin, S., & Adams, M. (2012). Security issues in cloud computing. In *Cloud Computing for Teaching and Learning: Strategies for Design and Implementation* (pp. 200-208). IGI Global.

[31]. Dewa, T., & Maglaras, L. A. (2016). Data mining and intrusion detection systems. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 7(1), 62-71.

[32]. Deyan, C., & Hong, Z. (2012, March). Data privacy and security protection issues in cloud computing. In *2012 International Conference on Computer Science and Electronics Engineering (ICCSEE)* (Vol. 1, pp. 647-651). IEEE.

[33]. Dhingra, M., Jain, S. C., & Jadon, R. S. (2021). Malicious node detection based on clustering techniques in network. *Materials Today: Proceedings*, *47*, 6676-6678.

[34]. Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M. (2010). Evaluating The Performance of Symmetric Encryption Algorithms. *International Journal of Network Security*, *10*(3), 216-221.

[35]. Feng, J., Chen, Y., Summerville, D., Ku, W. S., & Su, Z. (2011, January). Enhancing cloud storage security against roll-back attacks with a new fair multi-party non-repudiation protocol. In *2011 IEEE Consumer Communications and Networking Conference (CCNC)* (pp. 521-522). IEEE.

[36]. Fu, K., Ren, K., Shu, J., Sun, X., & Huang, F. (2016). Enabling personalized search over encrypted outsourced data with efficiency improvement. *IEEE Transactions on Parallel and Distributed Systems*, *27*(9), 2546-2559.

[37]. Fugkeaw, S. (2012, September). Achieving privacy and security in multi-owner data outsourcing. In *2012 Seventh International Conference on Digital Information Management (ICDIM)* (pp. 239-244). IEEE.

[38]. Ateniese, G., Burns, R., Curtmola, R., Herring, J., Khan, L., Kissner, A., ... & Song, D. (2007, October). Provable data possession at untrusted stores. In *Proceedings of the 14th ACM conference on Computer and communications security* (pp. 598-609).

[39]. Han, G., Qian, A., Jiang, J., Sun, N., & Liu, L. (2016). A grid-based joint routing and charging algorithm for industrial wireless rechargeable sensor networks. *Computer Networks*, *101*, 19-28.

[40]. Nadiammai, G. V., & Hemalatha, M. (2014). Effective approach toward Intrusion Detection System using data mining techniques. *Egyptian Informatics Journal*, *15*(1), 37-50.

[41]. Graf, S., Lang, P., Hohenadel, S. A., & Waldvogel, M. (2012, October). Versatile key management for secure cloud storage. In *2012 IEEE 31st Symposium on Reliable Distributed Systems (SRDS)* (pp. 469-474). IEEE.

[42]. Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding Cloud Computing Vulnerabilities. *Security & Privacy, IEEE*, 9(2), 50-57.

[43]. Guang, X., & Min, N. (2013, October). Anomaly intrusion detection based on wavelet kernel LS-SVM. In *2013 IEEE 3rd International Conference on Computer Science and Network Technology (ICCSNT)* (pp. 434-437). IEEE.

[44]. Guo, Y., Ping, N., Liu, S., & Luo, S. (2016). A two-level hybrid approach for intrusion detection. *Neurocomputing*, *214*, 391-400.

[45]. Ruan, H., Lin, C., Chen, Z., & Ni, J. (2006, November). Handling high speed traffic measurement using network processors. In *International Conference on Communication Technology* (pp. 1-4). IEEE.

[46]. Hamlen, K., Kantarcioglu, M., Khan, L., & Thuraisingham, B. (2012). Security issues for cloud computing. *International Journal of Information Privacy and Security*, *4*(2), 39-51.

[47]. Hardjono, T. (2005). *Security in wireless LANS and MANS*. Artech House Publishers.

[48]. Idrizi, F., Dalipi, F., & Rustemi, E. (2013). Analyzing the speed of combined cryptographic algorithms with secret and public key. *International Journal of Engineering Research and Development*, *8*(2), 45-48.

[49]. Itani, W., Kayssi, A., & Chehab, A. (2009, December). Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures. In *2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing* (pp. 711-716). IEEE.

[50]. Liu, J. D., Yan, B. H., Shenker, S., & Schapira, M. (2011, November). Data driven network connectivity. In *Proceedings of the 10th ACM Workshop on Hot Topics in Networks* (pp. 1-8).

[51]. Manoharan, J. J., Ganesh, S. H., & Sathiaseelan, J. G. R. (2016). Outlier detection using enhanced k-means clustering algorithm and weight based center. *App. Int. J. Comput. Sci. Mobile Co*, *5*(4), 453-464.

[52]. Lin, J. (2019). Accelerating Density Peak Clustering Algorithm (pp. 1-18).