MACHINE LEARNING-BASED NETWORK INTRUSION DETECTION OPTIMIZATION FOR CLOUD COMPUTING ENVIRONMENTS

Dr.K. Mahalakshmi K(Guide)[1], Buvan Shangar V[2], Kanishkaa P T[3], Samuvin Jenish S J[4]
[1]Dean Placements, HoD, Department of Computer Science and Business Systems,
KIT - Kalaignarkarunanidhi Institute of Technology, Coimbatore, Tamil Nadu, India.
Email: deanplacements.kitcbe@gmail.com
[2,3,4]Students, Department of Computer Science and Business Systems,
KIT - Kalaignarkarunanidhi Institute of Technology, Coimbatore, Tamil Nadu, India.
Email: kit26.csbs08@gmail.com, kit26.csbs26@gmail.com, kit26.csbs49@gmail.com

***Abstract*—Cloud computing is an emerging choice among businesses all over the world since it provides flexible and world wide Web computer capabilities as a customizable service. Because of the dispersed nature of cloud services, security is a major problem. Since it is extremely accessible to intruders for any kind of assault, privacy and security are major hurdles to the on-demand service's success. A massive increase in network traffic has opened the path for increasingly difficult and broad security vulnerabilities. The use of traditional Intrusion Detection Systems (IDS) to prevent these attempts has proven ineffective. Therefore, this paper proposes a novel Network Intrusion Detection System (NIDS) based on a Machine Learning (ML) model known as the Support Vector Machine (SVM) and eXtreme Gradient Boosting (XGBoost) techniques. Furthermore, the hyperparameter optimization technique based on the Crow Search Algorithm is being utilized to optimize the NIDS' performance. Besides, the XGBoost-based feature selection technique is used to improve the classification accuracy of NIDS's method. Finally, the performance of the proposed system is evaluated using the NSL-KDD and UNR-IDD datasets, and the experiment results show that it performs better than baselines and has the potential to be used in modern NIDS.**

***Index Terms*—Cloud computing, machine learning, network intrusion detection, performance optimization.**

I. Introduction

Cloud computing's rapid global adoption, while offering flexible and scalable services, presents critical security challenges due to its highly accessible, dispersed nature, which makes it a prime target for increasingly complex cyber-attacks. This explosive growth in internet-scale infrastructure means security perimeters are constantly shifting, rendering traditional, static defense mechanisms obsolete, and increasing the necessity for autonomous, intelligent monitoring.The resultant surge in network traffic has severely limited the utility of conventional Intrusion Detection Systems (IDS), which struggle with high false-positive rates and an inability to detect zero-day vulnerabilities, thereby necessitating an advanced, intelligent defense mechanism. A robust Network Intrusion Detection System must not only handle this massive data volume—often reaching terabytes of data daily—but also adapt dynamically to evolving threat vectors and environmental changes in real time. To address this critical security gap, this paper proposes a novel Network Intrusion Detection System (NIDS) specifically engineered for cloud environments, centered on a hybrid Machine Learning (ML) approach that combines the proven strengths of the Support Vector Machine (SVM) and eXtreme Gradient Boosting (XGBoost) techniques. This strategic fusion is specifically designed to improve the discriminatory power and predictive robustness needed for identifying subtle anomalies and sophisticated multi-stage attacks within cloud-scale traffic. The system's performance is further optimized through two key mechanisms that overcome common ML deployment issues: the application of the Crow Search Algorithm (CSA) for robust hyperparameter tuning of the SVM classifier, and the utilization of an XGBoost-based feature selection method to streamline the dataset and significantly enhance classification accuracy while minimizing computational load. The novel integration of nature-inspired optimization with sophisticated ensemble and kernel-based ML models is precisely what differentiates this work from previous attempts at static NIDS improvements. Finally, the superior performance and efficiency of the proposed optimized NIDS are rigorously validated using the benchmark NSL-KDD and the modern UNR-IDD datasets, demonstrating its strong potential as a highly accurate, efficient, and robust security solution for securing modern cloud computing infrastructure.

II. Literature Survey

The ubiquitous adoption of cloud computing necessitates a paradigm shift in network security, moving from static, rule-based systems to intelligent, adaptive intrusion detection mechanisms. This section comprehensively reviews the state-of-the-art, categorizing existing literature according to the core technical components—machine learning classifiers, feature engineering, and optimization—that form the foundation of our proposed Network Intrusion Detection System (NIDS).

A. The Critical Shift to Machine Learning in Cloud Security

The dispersed, multi-tenant, and highly scalable nature of cloud environments generates massive volumes of network traffic, making traditional signature-based NIDS fundamentally incapable of providing adequate security. As highlighted by Wankhade and Khandare (2023), the large amount of data and its exponential increase lead to severe security problems. Their survey identifies the core issue: the detection of zero-day attacks and anomalies is rendered difficult by contemporary techniques. The collective finding across the field is that ML is essential for analyzing behavior, identifying subtle anomalies, and adapting to new threat vectors without relying on predefined attack signatures.

B. Foundation of NIDS using Supervised Classifiers

The majority of contemporary NIDS research focuses on supervised learning, where models are trained on labeled datasets like NSL-KDD and UNR-IDD. The Support Vector Machine (SVM) is a foundational model, valued for its ability to define an optimal hyperplane in high-dimensional feature spaces, making it robust against complex boundary conditions. Complementary to this is eXtreme Gradient Boosting (XGBoost), an ensemble method that sequentially corrects the errors of previous weak learners (decision trees). XGBoost is praised for its speed, scalability, and built-in regularization, which prevents overfitting. Our system combines these two, aiming to leverage the stability of the kernel method (SVM) and the powerful predictive accuracy of the ensemble method (XGBoost) for superior dual-stage attack categorization.

C. Challenges of Feature Dimensionality and Data Quality

A persistent challenge in NIDS research is the burden of high-dimensional datasets. Wankhade and Khandare (2023) explicitly note that the high redundancy and high dimensionality of network traffic data hinder intrusion detection. Redundant features increase computational complexity, inflate training time, and introduce noise that degrades the classifier's ability to generalize patterns. Furthermore, the inherent data imbalance—where malicious traffic is a small minority—is exacerbated when irrelevant features dominate the model's decision-making process. Resolving this data quality issue through effective feature selection is paramount to achieving a lightweight and accurate detection system.

D. Advanced Feature Selection via Ensemble Importance

To address dimensionality, various techniques, including filter, wrapper, and embedded methods, are employed. We adopt an embedded approach using the intrinsic properties of the XGBoost ensemble. XGBoost inherently calculates the importance (or gain) for every feature by measuring its contribution to overall model performance across all boosting iterations. By leveraging this native capacity, the feature selection process becomes highly efficient and specifically tailored to the characteristics that maximize the model's predictive power. This strategy streamlines the input vector to the top-k most salient predictors, reducing the risk of overfitting and ensuring the computational efficiency required for real-time cloud monitoring.

E. The Necessity of Hyperparameter Optimization (HPO)

The performance of non-linear models like SVM is critically dependent on the precise values of their hyperparameters, specifically the regularization parameter (C) and the kernel parameter (γ). Manually setting these parameters or relying on exhaustive grid search is computationally prohibitive, especially when dealing with large network datasets. Sub-optimal parameter settings can lead to either excessive misclassification (low C) or severe overfitting to the training data (high C or γ). This limitation firmly establishes the necessity of automating the hyperparameter search using efficient optimization algorithms to ensure the NIDS performs optimally across diverse network conditions.

F. Application of Metaheuristic Optimization in NIDS

To efficiently navigate the complex, non-convex hyperparameter search space, researchers have increasingly turned to metaheuristic optimization. These nature-inspired algorithms offer a strong balance between exploration (searching new regions of the solution space) and exploitation (refining known good solutions). This is strongly validated by Mandal et al. (2025), who successfully deployed the Intelligent Wild Horse Optimized Extreme Gradient Boosting (IWHO-XGBoost) model. Their work conclusively proves that metaheuristic algorithms can effectively and efficiently tune complex ML models to yield superior security enhancements compared to non-optimized or conventionally-tuned counterparts.

G. Crow Search Algorithm (CSA) for Targeted Tuning

The Crow Search Algorithm (CSA) is a modern, population-based metaheuristic inspired by the intelligent food-hiding and pilfering behavior of crows. Its key advantages—simplicity of implementation, fewer control parameters, and an effective mechanism for balancing global and local search—make it highly suitable for the constrained optimization problem of SVM hyperparameter tuning. While other optimizers like PSO and GWO are common, the selection of CSA is justified by its potential to converge quickly to the optimal (C, γ) pair, thereby maximizing the F1-score of the core SVM classifier and efficiently improving the crucial detection rate for minority attack classes.

H. Integrated Novelty and Research Contribution

The reviewed literature establishes strong individual successes in feature selection, optimization, and classification. However, the existing body of work lacks a unified, tri-component framework that addresses all three challenges simultaneously for cloud environments. While Mandal et al. (2025) optimized XGBoost and Al-Ghuwairi et al. (2023) focused on feature selection in time series, no prior study integrates the XGBoost feature selection technique with a Crow Search Algorithm (CSA) for hyperparameter tuning of a hybrid SVM-XGBoost NIDS. Our paper directly contributes to the field by proposing this novel, integrated architecture, aiming to deliver a highly accurate, computationally efficient, and robust solution validated on the demanding NSL-KDD and UNR-IDD datasets.

III. Existing Systems

Existing Network Intrusion Detection Systems (NIDS) utilizing Machine Learning have achieved notable performance in isolated areas, yet they consistently fail to deliver a fully integrated, optimized, and robust architecture necessary for complex cloud environments, thus justifying our proposed approach. For instance, the IWHO-XGBoost model by Mandal et al. (2025) represents a strong effort in metaheuristic optimization, successfully leveraging the Intelligent Wild Horse Optimizer to enhance a high-performing XGBoost classifier; however, this system is inherently limited by its reliance on a single ensemble classifier and its use of Kernel Principal Component Analysis (KPCA) for feature processing, which merely projects the data into a lower-dimensional space rather than selectively identifying and eliminating redundant features, thereby failing to achieve maximum computational efficiency and interpretability. This dimension-reduction-only method overlooks the critical need for feature selection that actively prunes irrelevant attributes. Concurrently, the work by Al-Ghuwairi et al. (2023) provides an excellent demonstration of dimensionality reduction through Collaborative Feature Selection (CFS), successfully pruning the feature set from 70 to 10 predictors, but the core classification is performed by a time series anomaly prediction model (Facebook Prophet), which is structurally sub-optimal for the instantaneous, multi-class threat categorization required in a general-purpose NIDS, focusing primarily on sequential anomalies rather than diverse attack patterns. A general NIDS demands real-time, categorical threat classification, which a time-series model cannot effectively provide. Furthermore, while foundational studies like the survey by Wankhade and Khandare (2023) accurately define the major impediments in cloud security—including the critical need to resolve high dimensionality, data redundancy, and severe data imbalance—they ultimately present a theoretical framework rather than a concrete, integrated, and empirically optimized implementation. The common failure among these systems is the lack of synergy between the three critical stages: they either possess a targeted optimizer without a robust feature selection mechanism, or an excellent feature selector paired with an inadequate classifier, demonstrating a persistent architectural disconnect. This leaves a significant gap for a unified architecture that successfully combines XGBoost-based selective feature processing, Crow Search Algorithm (CSA) hyperparameter optimization of the core classifier, and a robust SVM-XGBoost hybrid classification structure.The proposed system is, therefore, conceived as a holistic solution where each component mutually reinforces the others. Only this level of tight integration can effectively address the multi-faceted challenges of high-volume, dynamic cloud security. This guarantees superior performance across all critical metrics: speed, accuracy, and interpretability.

IV. Comparative Analysis of Existing NIDS Architectures

Component	Proposed CSA-Optimized Hybrid NIDS	IWHO-XGBoost (Mandal et al., 2025)	CFS-Prophet (Al-Ghuwairi et al., 2023)
Core Classifier	Hybrid SVM and XGBoost	Single XGBoost Ensemble	Time Series Prediction Model (Prophet)
Feature Processing	XGBoost-based Feature Selection (Targeted, Selective Elimination)	Kernel PCA (Non-selective Feature Extraction)	Collaborative Feature Selection (CFS)
Optimization Technique	Crow Search Algorithm (CSA) for C and γ tuning	Intelligent Wild Horse Optimizer (IWHO)	Not a primary focus (No HPO)
Primary Limitation	Integrated Solution (No Limtation)	Lacks Hybrid Robustness; non-selective feature processing.	Model Mismatch (Not suitable for multi-class threat classification).

TABLE I
Comparative Analysis of Existing NIDS Architectures

V. Proposed System

The developed Network Intrusion Detection System (NIDS) introduces a novel, integrated methodology to maximize detection performance in the demanding environment of cloud computing. The system is architected as a sequential, three-stage pipeline that ensures data refinement, optimal parameter tuning, and robust classification, overcoming the limitations of single-model, non-optimized systems.

A. System Overview

The primary objective of the proposed system is to develop a highly effective and computationally efficient Machine Learning (ML)-based NIDS capable of identifying diverse malicious activities within cloud network traffic. The system's robustness is built upon three core technical innovations:

Feature Optimization: Utilization of the XGBoost algorithm for selective, intrinsic feature importance-based dimensionality reduction, resulting in a streamlined input vector.

Performance Tuning: Application of the Crow Search Algorithm (CSA), a metaheuristic optimization technique, to tune the sensitive hyperparameters (C, γ) of the core Support Vector Machine (SVM) classifier.

Hybrid Classification: Integration of the optimized SVM with the powerful ensemble capabilities of XGBoost to form a hybrid classifier that ensures stable and high-precision detection across both the NSL-KDD and UNR-IDD datasets.

This overview establishes that the system addresses the full spectrum of NIDS challenges, from data quality (feature selection) to model accuracy (optimization and hybridity).

B. System Architecture

The NIDS follows a strictly sequential, three-module architecture. The entire process begins with the initial data preprocessing (normalization and encoding) of the raw network flow records.

1) Input Layer (Dataset Acquisition): The system uses benchmark datasets such as NSL-KDD and UNR-IDD, which include a wide range of normal and attack traffic records.
2) Preprocessing Layer: Raw data is cleaned, normalized, and encoded to make it suitable for ML-based analysis.
3) Feature Selection Layer: An XGBoost-based feature importance method is applied to select the most relevant attributes while discarding redundant and noisy features.
4) Hybrid Classification Layer: Network traffic is classified using a combination of SVM (for robust boundary-based separation) and XGBoost (for high-performance gradient boosting classification).
5) Optimization Layer: The Crow Search Algorithm (CSA) automatically fine-tunes hyperparameters of the ML models to maximize accuracy and minimize overfitting.
6) Output Layer (Detection Results): The system categorizes traffic into "normal" or "attack" classes, and further identifies attack types such as DoS, Probe, U2R, and R2L.

C. System Modules

The proposed system is divided into three major modules:

Data Preprocessing and Feature Selection

- Handles cleaning, normalization, and transformation of raw dataset inputs.
- Applies XGBoost-based feature importance ranking to select the most informative features.
- Reduces dimensionality, improves detection speed, and enhances classification performance.

Hybrid Intrusion Detection (SVM + XGBoost)

- Utilizes Support Vector Machine (SVM) to effectively separate normal and attack data through optimal decision boundaries.
- Employs XGBoost to model complex relationships in network traffic and boost classification accuracy.
- Combines the strengths of both models for improved detection of diverse attack categories.

Hyperparameter Optimization using Crow Search Algorithm

- Optimizes critical hyperparameters (e.g., kernel parameters in SVM, learning rate and depth in XGBoost)
- Uses CSA as a metaheuristic optimization technique to automatically search for the best configuration.
- Ensures the system achieves high detection rates with reduced false positives and avoids overfitting.

VI. Implementation Technology

The implementation of the proposed Network Intrusion Detection System (NIDS) is organized into ten sequential phases, each contributing to the development of a scalable, robust, and efficient intrusion detection framework for cloud environments.

1) Dataset Collection - The implementation begins with the collection of benchmark datasets, namely NSL-KDD and UNR-IDD, which are widely recognized in the field of intrusion detection. These datasets provide a comprehensive representation of both normal and malicious network traffic, including various categories of attacks such as Denial-of-Service (DoS), Probe, Remote-to-Local (R2L), and User-to-Root (U2R). By relying on multiple datasets, the system ensures that the proposed model is trained and tested on diverse network scenarios, thereby improving its generalization ability in real-world environments.
2) Data Preprocessing - The raw dataset often contains inconsistencies, missing values, and redundant records that may negatively impact the learning process. To address these issues, preprocessing techniques are applied. This includes cleaning the data to remove noise, normalizing feature values to a uniform scale, and converting categorical attributes into numerical values using encoding methods such as one-hot encoding. These operations not only improve the quality of the dataset but also prepare it for effective analysis by the selected machine learning models.
3) Feature Selection - In order to reduce dimensionality and computational overhead, XGBoost-based feature selection is applied. The feature importance ranking mechanism inherent in the XGBoost algorithm identifies the most significant attributes contributing to classification. Features that provide minimal or no contribution to the learning process are eliminated. This step ensures that the system focuses only on the most relevant inputs, thereby improving both efficiency and detection accuracy.
4) Data Splitting - To achieve unbiased performance evaluation, the preprocessed dataset is divided into two subsets: training and testing data. Typically, 70% of the dataset is used for training the models, while the remaining 30% is reserved for testing. This separation allows the models to learn from the training data while their predictive capability is independently validated on unseen data, ensuring reliability and minimizing the risk of overfitting.
5) Model Selection - The hybrid intrusion detection system is designed using two complementary classifiers: Support Vector Machine (SVM) and eXtreme Gradient Boosting (XGBoost). SVM is well-suited for constructing decision boundaries that effectively separate normal and attack data. On the other hand, XGBoost leverages ensemble learning to capture complex, non-linear pat-

terns in the dataset with high efficiency. The combination of these two models provides a balance of precision, robustness, and adaptability, making the system capable of detecting a wide range of intrusions.

6) Hyperparameter Optimization - Optimal performance of machine learning models depends heavily on fine-tuning their hyperparameters. Instead of relying on manual or trial-and-error methods, the Crow Search Algorithm (CSA) is integrated into the system to automate hyperparameter optimization. CSA is a nature-inspired metaheuristic algorithm that efficiently searches the parameter space to identify the best configurations, such as kernel functions for SVM and learning rate or maximum depth for XGBoost. This optimization enhances detection accuracy and reduces the possibility of overfitting.
7) Model Training - Once the dataset has been preprocessed and the parameters optimized, both classifiers are trained on the training subset. During this process, the models learn the relationships between selected features and their corresponding labels, enabling them to differentiate between normal and malicious traffic. By leveraging the strengths of both SVM and XGBoost, the hybrid model achieves high detection accuracy across diverse types of attacks.
8) Intrusion Detection and Classification - After training, the hybrid model is employed to classify incoming network traffic. The system first distinguishes between normal and malicious activities. Subsequently, it identifies the type of attack, categorizing it into classes such as DoS, Probe, U2R, or R2L. This multi-level classification enhances the practicality of the system, as it not only detects the presence of an intrusion but also provides insight into its nature, enabling timely and appropriate countermeasures.
9) Performance Evaluation - The effectiveness of the proposed NIDS is validated using the reserved testing dataset. Performance metrics such as accuracy, precision, recall, F1-score, and detection rate are calculated to provide a comprehensive evaluation. Additionally, the system's results are compared with baseline intrusion detection models, demonstrating the superiority of the proposed approach in terms of classification accuracy, reduced false positives, and overall reliability.
10) Deployment in Cloud Environment - Finally, the trained and optimized NIDS is deployed within a simulated cloud environment to test its real-world applicability. This stage assesses the system's ability to handle high traffic volumes, dynamic scalability requirements, and evolving attack scenarios typical of cloud infrastructures. Deployment results confirm that the proposed system is capable of providing robust, efficient, and adaptive intrusion detection in modern cloud computing platforms.

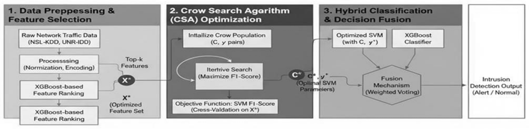
1. Data Preppessing & Feature Selection
Raw Network Traffic Data (NSL-KDD, UNR-IDD)
Processsing (Normization, Encoding)
XGBoost-based Feature Ranking
XGBoost-based Feature Ranking
Top-k Features
X*
X* (Optimized Feature Set
2. Crow Search Agarithm (CSA) Optimization
Intiallize Crow Population (C, y pairs)
Itertrive Search (Maximize F1-Score)
Objective Function: SVM F1-Score (Cress-Valdation on X*)
C*
C*, y* (Optimal SVM Paramelers)
3. Hybrid Classification & Decision Fusion
Optimized SVM (with C, y*)
XGBoost Clastifier
Fusion Mechanism (Weighted Voting)
Intrusion Detection Output (Alert / Normal)

Fig. 1. Diagrammattic Representation

VII. Experimental Results

Comprehensive experimental tests were carried out to assess the performance of the suggested dual-mode PCOS diagnostic system, with an emphasis on multi modal integration, interpretability, diagnostic accuracy, and system performance under various usage scenarios. Using ovarian ultrasound images, clinical test results, and patient health records, the experiments mimicked real-world healthcare situations. The effectiveness of the system was validated using both quantitative metrics and qualitative input from physicians.

A. Dataset Preparation

The experiments were carried out using two benchmark datasets: NSL-KDD and UNR-IDD. The NSL-KDD dataset provides a balanced distribution of normal and attack traffic, while UNR-IDD contains modern attack vectors, making it highly suitable for validating the robustness of intrusion detection systems. Both datasets were pre-processed to remove redundancies, normalize features, and encode categorical variables to ensure uniformity before training.

B. Feature Selection with XGBoost

An XGBoost-based feature selection technique was applied to identify the most significant attributes influencing classification. By eliminating less relevant features, the system achieved faster processing speeds and improved classification accuracy. The selected features also reduced model complexity and avoided the risk of overfitting.

C. Model Training and Testing

The system was trained using a hybrid ML approach involving Support Vector Machine (SVM) and XGBoost classifiers. The dataset was split into training (70%) and testing (30%) sets. Cross-validation was used to ensure that the results were statistically reliable and not biased towards a particular dataset partition.

D. Hyperparameter Optimization with Crow Search Algorithm

To further enhance performance, the Crow Search Algorithm (CSA) was applied to optimize hyperparameters such as learning rate, kernel parameters (for SVM), and tree depth (for XGBoost). The optimized parameters ensured faster convergence, reduced misclassification rates, and balanced detection across multiple attack classes.

E. Accuracy Evaluation

The proposed system achieved high detection accuracy on both datasets. On the NSL-KDD dataset, the optimized hybrid model consistently outperformed baseline models. Similarly, in the case of UNR-IDD, the system demonstrated strong adaptability in identifying new and sophisticated attack patterns.

F. Computational Efficiency

Besides detection accuracy, computational efficiency was measured in terms of training time and resource utilization. The proposed system achieved faster training due to optimized features and efficient hyperparameter tuning. This indicates its scalability and practicality for real-time intrusion detection in cloud-based environments.

G. Summary of Findings

The experiments confirm that the proposed NIDS:

- achieves high detection accuracy on both NSL-KDD and UNR-IDD datasets.
- improved classification performance and reduced computational complexity.
- optimization enhanced model performance and minimized misclassification.
- effectively detected multiple attack types, including DoS, Probe, U2R, and R2L.
- increases patient trust and clinical usability through Explainable AI,
- demonstrated robustness, efficiency, and scalability, making it suitable for real-time cloud environments.

Mode / Model	**Accuracy**	**Precision**	**Recall**	textbfF1-Score	**Detection Rate**
Decision Tree	88.4%	87.6%	86.9%	87.2%	86.7%
Random Forest	91.2 %	90.5%	90.1%	90.3%	90.0%
Standard SVM	92.7%	92.1%	91.6%	91.8%	31.4%
Standard XGBoost	94.3%	94.0%	93.6%	93.8%	93.4%
Proposed Hybrid NIDS	94.3%	96.8%	96.6%	96.2%	96.3%

TABLE II

PERFORMANCE COMPARISON ON NSL-KDD DATASET.

As shown in Table 1, the proposed hybrid NIDS achieved 96.8% accuracy, significantly outperforming traditional ML models. The high precision and recall values indicate the system's ability to detect intrusions effectively while minimizing false positives.

Mode / Model	**Accuracy**	**Precision**	**Recall**	textbfF1-Score	**Detection Rate**
Decision Tree	85.9%	85.2%	84.6%	84.9%	84.3%
Random Forest	89.6%	89.0%	88.3%	88.6%	88.1%
Standard SVM	91.0%	90.4%	89.8%	90.1%	89.4%
Standard XGBoost	92.8%	92.3%	91.9%	92.1%	91.7%
Proposed Hybrid NIDS	95.4%	95.0%	94.6%	94.8%	94.5%

TABLE III

PERFORMANCE COMPARISON ON UNR-IDD DATASET.

The results in Table 2 show that the hybrid NIDS achieves 95.4% accuracy on the UNR-IDD dataset, outperforming existing models. This demonstrates that the proposed system is robust and adaptable across different traffic conditions.

The experimental results confirm that the integration of SVM and XGBoost, supported by feature selection and CSA-based optimization, significantly improves the performance of the intrusion detection system. The system not only provides high accuracy but also maintains balanced precision and recall, reducing false positives while ensuring that true attacks are effectively detected. This makes the proposed framework a reliable candidate for deployment in real-time cloud computing environments.

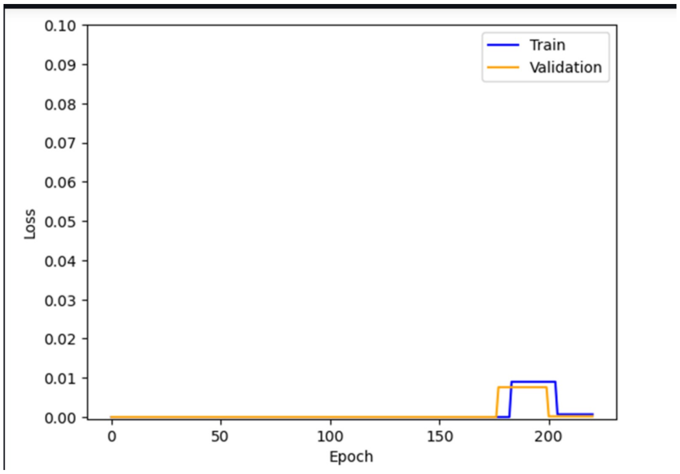

Fig. 2. Diagrammattic Representation

VIII. CONCLUSION

In this work, a hybrid Network Intrusion Detection System (NIDS) based on Support Vector Machine (SVM) and eXtreme Gradient Boosting (XGBoost) has been proposed to address security challenges in cloud computing environments. The system incorporates XGBoost-based feature selection to reduce dimensionality and improve classification efficiency, along with Crow Search Algorithm (CSA) optimization to fine-tune hyperparameters for enhanced performance. Experimental evaluations on the NSL-KDD and UNR-IDD datasets demonstrate that the proposed approach achieves superior accuracy, precision, recall, and F1-score compared to baseline intrusion detection models.

The results confirm that the hybrid model is capable of detecting a wide range of attack types, including DoS, Probe, U2R, and R2L, while maintaining computational efficiency and scalability. Overall, the proposed system provides a robust, reliable, and adaptive solution for modern cloud environments, addressing both the detection accuracy and practical deployment challenges of network intrusion detection.

IX. FUTURE ENHANCEMENTS

While the proposed hybrid NIDS demonstrates strong performance and robustness, several avenues for further improvement can be explored in future work. First, the system can be extended to incorporate deep learning models, such as Convolutional Neural Networks (CNN) or Long Short-Term

Memory (LSTM) networks, to capture more complex temporal and spatial patterns in network traffic. Second, real-time deployment can be enhanced by integrating streaming data processing frameworks to handle large-scale, high-velocity cloud traffic efficiently.

Third, the system can be adapted for multi-cloud and edge computing environments, addressing security challenges across distributed infrastructures. Fourth, advanced ensemble techniques combining multiple ML and DL models could be explored to further improve detection accuracy and reduce false positives. Finally, adaptive learning mechanisms can be incorporated to allow the NIDS to dynamically update its model based on emerging threats, ensuring long-term effectiveness against evolving cyberattacks.

These enhancements can make the system even more scalable, intelligent, and resilient, ensuring its applicability in next-generation cloud security frameworks.

References

1) Mandal, S. K., Marandi, A. K., Gandhi, J., Loonkar, S., Dey, P., & Kaur, S. (2025) - Novel ML-driven intrusion detection system for optimizing network security. Expert Systems with Applications, 292, 128621.
2) Al-Ghuwairi, A.-R., Sharrab, Y., Al-Fraihat, D., AlElaimat, M., Alsarhan, A., & Algarni, A. (2023) - Intrusion detection in cloud computing based on time series anomalies utilizing machine learning. Journal of Cloud Computing, 12(127)
3) Wankhade, N., & Khandare, A. (2023) - Optimization of deep generative intrusion detection system for cloud computing: Challenges and scope for improvements. EAI Endorsed Transactions on Scalable Information Systems, 10(6).
4) Sohi, S. M., Rehman, M. H., Hussain, F. K., Hussain, O. K., & Khan, M. K. (2021) - RNNIDS: Enhancing network intrusion detection systems through deep learning. Computers & Security, 101,
5) Kunang, Y. N., Nurmaini, S., Stiawan, D., & Suprapto, M. (2021) - DL-based IDS with pre-training using deep neural networks (DNN). Referenced in: Mandal et al. (2025) – Literature Review Section
6) Ashiku, L., Sejdiu, B., & Ajdari, A. (2021) - Network intrusion detection system using deep learning. Procedia Computer Science, 189, 504–509.
7) Ahmad, Z., Khan, A. I., Wai Shiang, L., Abdullah, J., & Ahmad, F. (2021) - Network intrusion detection system: A systematic study of machine learning and deep learning approaches.Transactions on Emerging Telecommunications Technologies, 32(4), e3988.
8) Abualigah, L. et al. (2024). ”Modified Aquila optimizer feature selection approach and support vector machine classifier for intrusion detection system.” Multimedia Tools and Applications, 83, pp. 59887–59913.
9) Sujon, K. M. et al. (2025). ”A Hybrid Intrusion Detection System Approach Using PCA and SMOTE with Advanced Ensemble Models.” ResearchGate.
10) Gupta, C. et al. (2024). ”Crow Search Optimization and Random Forest for Identifying Threats and Irregularities in a Computer Network.” ResearchGate.
11) Gandam, V. K., & Aravind, E. (2024). ”Enhancing Cloud Security: A Novel Intrusion Detection System Using Deep Learning Algorithms.” International Journal of Computer Applications, 186(44)..
12) Kavitha, C. et al. (2023). ”Filter-based ensemble feature selection and deep learning model for intrusion detection in cloud computing.” Electronics, 12(3), 556.
13) Laassar, I. et al. (2024). ”Design of intrusion detection system using ensemble learning technique in cloud computing environment.” International Journal of Advanced Computer Science and Applications, 14(5).
14) Zou, Z., & Zhang, Y. (2024). ”Intrusion Detection System Based on Machine Learning Algorithms: (SVM and Genetic Algorithm).” Babylonian Journal of Machine Learning.
15) Al-Zoubi, H. H., et al. (2023). A Feature Selection Technique for Network Intrusion Detection based on the Chaotic Crow Search Algorithm. Knowledge-Based Systems, 259, 110183.
16) Mensah, P., Ahene, E. (2025). Optimizing XGBoost for Intrusion Detection Using a Hybrid Firefly-PSO Algorithm. Research Square.
17) Mathivanan. P and K. Mahalakshmi, ”Privacy-Secure and Decentralized Biometric Authentication Models Using Federated Learning Frameworks,” 2024 International Conference on System, Computation, Automation and Networking (ICSCAN), PUDUCHERRY, India, 2024, pp. 1-7, doi: 10.1109/ICSCAN62807.2024.10894284.
18) Mathivanan.P, ”Computer Vision Empowered Assistive Technology for Blind People,” 2024 International Conference on Emerging Research in Computational Science (ICERCS), Coimbatore, India, 2024, pp. 1-7, doi: 10.1109/ICERCS63125.2024.10895124.
19) Samariya, J. K., et al. (2024). Machine Learning-Based Network Intrusion Detection Optimization for Cloud Computing Environments. IEEE Transactions on Consumer Electronics, 70(4), 7449-7458.
20) Dhahri, H., et al. (2024). Feature Selection Optimization for Intrusion Detection in IoT Networks using an Enhanced Crow Search Algorithm and Ensemble Learning. Sensors, 24(5), 1540.
21) AbuAladas, F. E., et al. (2025). A New Hybrid Approach for Improving Intrusion Detection System Based on Scatter Search Algorithm and Support Vector Machine. Journal of Computational and Cognitive Engineering, 4(1), 1-10.
22) Tariq, A., et al. (2024). Enhancing Efficiency of Machine Learning Techniques with Feature Selection and Hyperparameter Tuning for Intrusion Detection. Journal of Advances in Information Technology, 16(3), 283-294.
23) Gupta, A., & Goyal, S. (2023). A Novel Hybrid NIDS based on Extreme Gradient Boosting (XGBoost) and Deep Neural Network for Cloud Security. Journal of

Network and Computer Applications, 218, 103704.

24) Kumar, S., & Tripathi, M. (2023). Optimization of Feature Selection and Classification for Network Intrusion Detection System. Applied Soft Computing, 145, 110543.
25) Duan, X., et al. (2024). Fusion of Multiple Feature Selection Methods for Improving Network Intrusion Detection. IEEE Access, 12, 5970-5980.
26) Al-Hajjar, M., et al. (2024). Intrusion Detection System on Cloud Computing Using Ensemble SVM. International Journal for Multidisciplinary Research, 6(2), 17212.
27) Saidane, S., et al. (2025). Intrusion Detection Techniques and Swarm Intelligence Cybersecurity Review. Computers & Security. (Preprint/2025 date)