International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 05 Issue: 03 | March – 2026 DOI: 10.55041/ISJEM05574
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

A Survey Paper on a Double Layered Approach for detecting network intrusions

Balasani Avinash[1], Garisapati Sai Uday[2], Banoth Arun [3], Ramisetti Vallabharayudu[4]

[1]Assistant Professor of Department of CSE (AI & ML) of ACE Engineering College, India.

[2,3,4] Students of Department CSE (AI & ML) Of ACE Engineering College, India.

1. ABSTRACT

• This project presents a **Double-Layered Hybrid Approach (DLHA)** for **Network Intrusion Detection**. The system combines a **signature-based method** with **machine learning techniques** to accurately identify both **known attacks** and **rare anomalies**. During the project, we applied **Principal Component Analysis (PCA)** to extract the most significant features from the **NSL-KDD dataset**, capturing the common characteristics of different attack categories. In the **first layer**, a **Naive Bayes classifier** detects **Denial-of-Service (DoS)** and **Probe** attacks. In the **second layer**, a **Support Vector Machine (SVM)** separates **rare attacks** from normal traffic. The approach was trained, tested, and evaluated to measure **detection rate**, **accuracy**, and **false positive reduction**, showing improved performance compared to single classifiers.

Keywords:

• Network Intrusion Detection, Hybrid Approach, Machine Learning, Principal Component Analysis (PCA), Naive Bayes, Support Vector Machine (SVM), NSL-KDD Dataset.

2. INTRODUCTION

The Network security protects computer networks from unauthorized access, misuse, or damage, ensuring that data remains confidential, accurate, and available. As networks handle sensitive information, they face constantly evolving threats that traditional tools like firewalls or antivirus software cannot fully stop. To strengthen protection, Network Intrusion Detection Systems (NIDS) are used to monitor network traffic and identify suspicious or harmful activities that may slip past basic defenses. This project proposes a double-layered approach to enhance intrusion detection and offer stronger security against modern, complex attacks.

The first layer of the proposed model focuses on filtering and classifying network traffic into normal and suspicious categories. This preliminary screening reduces unnecessary processing and ensures faster response times. By eliminating clearly legitimate traffic early, the system improves efficiency and reduces computational overhead in the second layer.

The second layer performs deeper inspection using advanced classification algorithms to precisely categorize detected intrusions into specific attack types such as DoS, Probe, R2L, and U2R. This detailed analysis helps administrators understand the nature of the attack and take appropriate mitigation measures quickly.

3. BACKGROUND OF THE PROJECT

With the rapid growth of internet usage, cloud computing, and IoT devices, computer networks have become more complex and widely distributed. Organizations depend heavily on digital communication and online services to store, process, and transmit sensitive information. As a result, the risk of cyberattacks has increased significantly. Attackers continuously develop advanced techniques to exploit vulnerabilities in network infrastructure, applications, and protocols. Traditional security mechanisms such as firewalls, encryption, and antivirus software primarily focus on preventing unauthorized access and blocking known threats. However, these tools are often insufficient against sophisticated attacks such as Distributed Denial of Service (DDoS), phishing-based intrusions, insider threats, and zero-day exploits. Many

attacks bypass perimeter defenses and operate within the network, making detection more challenging. To overcome this drawback, anomaly-based detection techniques were developed. These methods establish a baseline of normal network behavior and detect deviations from it. Recently, machine learning and artificial intelligence have been widely adopted in IDS development to improve detection accuracy, adaptability, and automation. Machine learning models can learn complex patterns from large datasets and classify network traffic more effectively than rule-based systems.

4. LITERATURE REVIEW

1. Kajal & Nandal (2020):

The Genetic Algorithm for feature selection, DWT + ABC for preprocessing, hybrid ANN-SVM classifier and **Genetic Algorithm (GA)** is employed for optimal feature selection. Network intrusion datasets often contain a large number of redundant and irrelevant features, which can negatively impact model accuracy and increase processing time. GA, inspired by the principles of natural selection and evolution, searches for the most informative subset of features by applying operations such as selection, crossover, and mutation.

2. ElSayed, Le-Khac, Albahar, Jurcut (2021):

The CNN component automatically extracts deep spatial features from SDN traffic flows, reducing dependency on manual feature engineering and improving detection of complex attack patterns. The model leverages the centralized control plane of SDN to collect global traffic statistics, enabling more accurate and real-time intrusion detection compared to traditional distributed networks.

3. Das & Gündüz (2019):

Combining CNN with SVM, KNN, and Random Forest improves decision reliability through ensemble learning, reducing false positives and false negatives.The model was validated on multiple datasets (e.g., NSL-KDD, CIC-IDS2018, UNSW-NB15), demonstrating consistent performance and robustness under diverse traffic condition

4. Qazi, Faheem, Zia (2023):

The hybrid framework shows improved detection capability for unseen attacks by learning generalized traffic representations rather than relying only on known signatures. Feature optimization and regularization reduce unnecessary parameters, lowering computational cost while maintaining high detection accuracy. Achieved 98.9% accuracy on CICIDS-2018 dataset; captured both spatial and temporal attack patterns; handled class imbalance

5. ElSayed et al. (2021):

ElSayed and colleagues proposed a hybrid CNN-based intrusion detection model for Software Defined Networks (SDNs). Their framework integrates deep feature extraction with machine learning classifiers to enhance detection accuracy. They also introduced a novel regularization technique (SD-Reg) to minimize overfitting and improve model generalization across multiple benchmark datasets.

6. Le-Khac et al. (2020):

Le-Khac focused on big data analytics for cybersecurity applications. Their work emphasized scalable intrusion detection mechanisms capable of processing high- volume network traffic. They highlighted the importance of anomaly detection models in identifying zero-day and unknown attacks in dynamic network environments. The model incorporates an innovative SD-Reg regularization technique to control overfitting and improve generalization across multiple benchmark datasets such as NSL-KDD, CIC-IDS2018, and UNSW-NB15.

7. Singh and Sharma (2022):

Singh and Sharma proposed an optimized feature selection technique using Genetic Algorithms (GA) for intrusion detection systems. Their model reduced dimensionality and improved classification efficiency by selecting only the most relevant traffic features, leading to enhanced detection accuracy. the framework was designed to utilize the centralized control architecture of SDN, enabling efficient traffic monitoring and faster anomaly detection. By extracting flow-based

features directly from the SDN controller, the system ensures real-time detection with minimal latency. The researchers also addressed scalability concerns by optimizing model parameters and reducing computational complexity, making the system suitable for large-scale cloud and enterprise networks. Their cross-dataset validation confirmed robustness and adaptability under diverse traffic conditions. Furthermore, the hybrid model demonstrated resilience against imbalanced datasets and evolving cyber threats, highlighting its practicality for real-world deployment.

8. **Zhang et al. (2023):**

The study Zhang and team proposed an Artificial Bee Colony (ABC) optimization algorithm for tuning IDS parameters. The ABC-based optimization improved convergence speed and enhanced classifier performance, particularly in detecting complex and rare attack patterns.

9. Aljawarneh et al. (2018):

Aljawarneh and colleagues proposed a hybrid intrusion detection framework combining data preprocessing, feature selection, and machine learning classification. Their study emphasized reducing false alarm rates and improving detection of both known and unknown cyberattacks in large-scale networks.

5. COMPARISION TABLE

S. No	Author(s)	Title	Methodology	Key Contribution
1	Kajal & Nandal (2020	A hybrid approach for cyber security: improved intrusion detection system using ANN-SVM	Genetic Algorithm for feature selection, DWT + ABC for preprocessing, hybrid ANN-SVM classifier.	High detection accuracy (98.24%) and precision (99.6%) for DDoS; reduced false positives.
2	ElSayed, Le-Khac, Albahar, Jurcut (2021)	A novel hybrid model for intrusion detection systems in SDNs based on CNN and a new regularization technique	Hybrid model combining CNN with SVM, KNN, and RF; introduced SD-Reg regularizer to reduce overfitting	Achieved 85.2% accuracy; effectively detected low-frequency attacks; ensemble outperformed individual classifiers
3	Gao, Shan, Hu, Niu, Liu (2019)	An Adaptive Ensemble Machine Learning Model for Intrusion Detection	Ensemble approach with Decision Trees, Random Forest, KNN, DNN, and adaptive voting	Achieves high accuracy in predicting student success and improving adaptive outcomes.

4	Das & Gündüz (2019)	An Adaptive Ensemble Machine Learning Model for Intrusion Detection	Ensemble approach with Decision Trees, Random Forest, KNN, DNN, and adaptive voting	Achieved 85.2% accuracy; effectively detected low-frequency attacks; ensemble outperformed individual classifiers
5	Das & Gündüz (2019)	Analysis of cyber-attacks in IoT-based critical infrastructures	Survey of IoT-based attacks on critical infrastructures; categorized threats and strategies	Highlighted vulnerabilities in energy, transport, and communication systems; stressed need for IDS in IoT
6	Qazi, Faheem, Zia (2023)	Hybrid Deep-Learning-Based Network Intrusion Detection System	CNN + RNN hybrid IDS; flow-based statistical analysis; preprocessing with one-hot encoding	Achieved 98.9% accuracy on CICIDS-2018 dataset; captured both spatial and temporal attack patterns; handled class imbalance
7	Zhang et al. (2023)	Swarm Intelligence–Optimized Intrusion Detection System	Applied Artificial Bee Colony (ABC) optimization to enhance feature selection and classifier parameter tuning for improved intrusion detection efficiency.	Improved detection accuracy, reduced false positives, and achieved faster optimization convergence compared to conventional techniques
8	Aljawarneh et al. (2018)	Hybrid Machine Learning Framework for Network Intrusion Detection	Developed a hybrid IDS combining effective preprocessing, feature selection, and supervised machine learning algorithms	Enhanced classification accuracy and significantly reduced false alarm rates across diverse attack types.

9	Singh and Sharma (2022)	Genetic Algorithm–Driven Feature Optimization for IDS	Utilized Genetic Algorithm (GA) to identify the most relevant traffic features to improve classifier performance and reduce dimensionality.	Achieved higher precision and recall with reduced computational complexity and training time.
10	García-Mateos et al. (2020)	Automated Code Assessment Systems: A Systematic Review	Surveys sandboxed execution, test-case evaluation, and	Establishes best practices for scalable, reliable

6. System Architecture

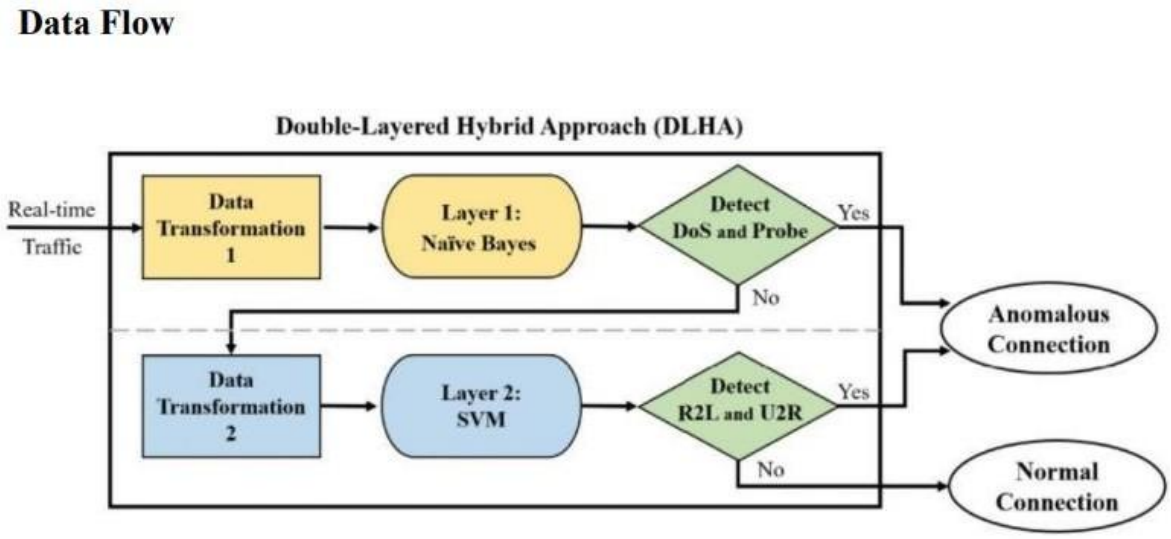

Fig 1 : System Architecture

7. ResearchGaps Addressed:

Limitations of Single-Layer Detection Systems

o Most traditional Intrusion Detection Systems rely on a single detection mechanism, such as signature-based, anomaly-based, or standalone machine learning models. While these approaches are effective in controlled environments, they exhibit significant limitations in real-world network scenarios. Signature-based systems are incapable of detecting zero-day or previously unseen attacks.

Poor Handling of Imbalanced and Complex Attack Patterns

o Network intrusion datasets are inherently imbalanced, where normal traffic instances significantly outnumber attack samples, and certain attack types such as User-to-Root (U2R) and Remote-to-Local (R2L) appear rarely. Many conventional systems become biased toward majority classes, leading to poor detection performance for minority but critical attack categories. Additionally, complex multi-stage attacks are difficult to capture using a single detection model..

Hybrid Intelligence Integration

o Existing intrusion detection frameworks typically depend on either statistical methods, traditional machine learning algorithms, or deep learning techniques independently. However, relying on a single paradigm often results in performance trade-offs between accuracy, interpretability, and computational efficiency. The proposed double-layered system integrates hybrid intelligence by combining a fast and lightweight preliminary detection layer with a more advanced and computationally intensive classification layer. This integration ensures both rapid detection and precise categorization.

Scalability and Real-Time Constraints

o Real-time intrusion detection requires systems to process large volumes of network traffic with minimal latency. Deep learning models, although highly accurate, demand significant computational resources, making them challenging to deploy in high-speed network environments. The double-layered architecture improves scalability by assigning simple filtering tasks to the first layer and reserving complex analysis for the second layer only when necessary. This selective deep inspection reduces computational overhead, enhances processing speed, and ensures the feasibility of real-time deployment without compromising detection accuracy.

Advantages of the Double-Layered Architecture

o The double-layered intrusion detection framework offers several advantages over conventional single-layer systems. It reduces false positive rates by refining suspicious traffic through an additional verification stage, improves detection of minority attack classes, and balances speed with accuracy. The modular design allows independent optimization of each layer, making the system adaptable to various network environments and datasets. Overall, this structured approach enhances detection performance, resource efficiency, and resilience against evolving cyber threats.

Integrated Double-Layered Detection Framework

o Traditional intrusion detection systems often rely on a single detection mechanism, which limits their ability to balance speed, accuracy, and adaptability. The proposed double-layered detection framework addresses this gap by introducing a hierarchical structure in which the first layer performs rapid coarse-grained filtering to distinguish normal traffic from suspicious activity, while the second layer conducts fine-grained classification of identified threats. This layered design reduces false positives, improves detection of rare and complex attack patterns, and enhances real-time performance.

8. PROPOSED SYSTEM

This work introduces a Double Layered Hybrid Approach (DLHA) for intrusion detection that combines efficiency with high classification accuracy. In the first layer, a Naïve Bayes classifier is employed to perform rapid filtering of common network attacks such as Denial of Service (DoS) and Probe attacks. Due to its probabilistic foundation and low computational complexity, Naïve Bayes enables fast screening of high-volume network traffic with minimal resource consumption. Traffic identified as suspicious is then forwarded to the second layer, where a Support Vector Machine (SVM) performs refined classification. The SVM focuses particularly on detecting rare but critical intrusions such as Remote-to-Local (R2L) and User-to-Root (U2R) attacks, which are often difficult to identify due to class imbalance and subtle behavioral patterns.

For training and evaluation, the NSL-KDD dataset is utilized, as it provides a balanced representation of attack categories and reduces redundancy present in earlier datasets. To enhance model performance and computational efficiency, Principal Component Analysis (PCA) is applied for feature reduction, maximizing variance while lowering dimensionality. Overall, this layered pipeline ensures efficient processing of high-volume network traffic while maintaining strong precision and sensitivity in detecting rare and sophisticated cyber threats.

9. CONCLUSION AND FUTURE SCOPE

The proposed Double Layered Hybrid Approach (DLHA) for intrusion detection demonstrates an effective balance between computational efficiency and detection accuracy. By integrating a Naïve Bayes classifier in the first layer for rapid filtering of common attacks and a Support Vector Machine (SVM) in the second layer for refined classification of rare and critical intrusions, the system successfully addresses the limitations of traditional single-layer IDS models. The use of the NSL-KDD dataset ensures reliable evaluation with balanced attack representation, while Principal Component Analysis (PCA) enhances performance through dimensionality reduction and improved classifier efficiency. Overall, the layered architecture reduces false positives, improves detection of minority attack classes such as R2L and U2R, and ensures scalability for high-volume network traffic, making it suitable for practical real- time deployment scenarios.

In the future, the system can be extended by integrating deep learning techniques such as LSTM or CNN models to capture temporal and spatial patterns in network traffic. The inclusion of real-time streaming data and deployment in cloud or IoT environments can further validate its practical applicability. Additionally, incorporating adaptive learning mechanisms would enable the model to dynamically update itself against emerging and zero-day attacks. Expanding the evaluation to more recent and diverse datasets, as well as integrating explainable AI techniques for better interpretability, can further enhance the robustness, transparency, and real-world usability of the proposed intrusion detection framework.

10.REFERENCES

1. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A Detailed Analysis of the KDD CUP 99 Dataset. *Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications.*

2. Marina, Lippmann, R. P., Fried, D. J., Graf, I., et al. (2000). Evaluating Intrusion Detection Systems: The 1998 DARPA Off-Line Intrusion Detection EvaluationMukkamala, S., Sung, A. H., & Abraham, A. (2005). Intrusion Detection Using Ensemble of Soft Computing Paradigms. *Proceedings of the International Conference on Fuzzy Systems.*

3. Panda, M., & Patra, M. R. (2007). Network Intrusion Detection Using Naïve Bayes.

International Journal of Computer Science and Network Security.

4. Wang, W., Sheng, Y., Wang, J., et al. (2017). HAST-IDS: Learning Hierarchical Spatial-Temporal Features Using Deep Neural Networks to Improve Intrusion Detection. *IEEE Access.*

5. Kim, G., Lee, S., & Kim, S. (2014). A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection. *Expert Systems with Applications.*

6. Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials.*

7. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. *IEEE Access*

8. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. *Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP).*

9. Sahu, S., & Mehtre, B. M. (2015). Network Intrusion Detection System Using J48 Decision Tree. *Proceedings of the International Conference on Advances in Computing, Communications and Informatics.*