International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802039

Hybrid Intrusion Detection System for Enhanced SME Network Security

Mr.R.Krishnakumar[1], Mr.K.Aravinthkumar[2], Mr.G.Gokul Priyan[3], Mr.Aathina Srinath[4], Mr.Abhinav Raj[5]

AP, Department of CSE, Gnanamani College of Technology, Namakkal, Tamil Nadu, India[1]

UG Scholars, Department of CSE, Gnanamani College of Technology, Namakkal, Tamil Nadu, India[2-5]

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT: The rapid increase in the complexity and volume of cyber threats has created an urgent need for intelligent and adaptive Intrusion Detection Systems (IDS) to secure modern digital infrastructures, particularly within Small and Medium Enterprises (SMEs). Conventional IDS mechanisms, primarily based on signature matching and static rule sets, are inadequate for identifying zero-day attacks and evolving intrusion patterns. To overcome these limitations, Artificial Intelligence (AI) has emerged as a powerful enhancement for IDS frameworks. AI-driven IDS integrate Machine Learning (ML) techniques to analyze large-scale network traffic, system logs, and user behavior data, enabling accurate detection of anomalous and malicious activities.

Recent advancements in ensemble learning algorithms have significantly improved detection performance and system adaptability. In particular, Extreme Gradient Boosting (XGBoost) enables efficient classification by minimizing prediction errors through iterative learning and feature optimization. Additionally, intelligent data preprocessing and feature engineering techniques enhance model robustness and reduce false positive rates. The integration of adaptive learning mechanisms further strengthens the system's ability to respond dynamically to emerging threat patterns in real time.

This paper presents a hybrid AI-driven intrusion detection framework designed for SME network environments. The proposed system leverages XGBoost-based classification to improve detection accuracy while maintaining computational efficiency. Experimental evaluation demonstrates superior performance compared to conventional IDS approaches.

KEYWORDS: Hybrid Intrusion Detection System, Artificial Intelligence, Machine Learning, XGBoost, Network Security, SME Cybersecurity, Anomaly Detection, Adaptive Learning, Cyber Threats, Intelligent Security Systems

I. INTRODUCTION

The rapid digitalization of businesses and industrial systems has significantly increased the exposure of network infrastructures to sophisticated cyber threats, including data breaches, ransomware attacks, and Advanced Persistent Threats (APTs). Small and Medium Enterprises (SMEs), in particular, face heightened vulnerability due to limited cybersecurity resources and reliance on conventional protection mechanisms. Traditional Intrusion Detection Systems (IDS), which primarily depend on signature-based and rule-based detection strategies, are often ineffective in identifying zero-day attacks and polymorphic malware. These limitations highlight the urgent need for intelligent and adaptive security solutions capable of responding to dynamic threat environments.

Artificial Intelligence (AI) has emerged as a transformative approach for enhancing IDS performance by enabling systems to learn from historical data, recognize complex behavioral patterns, and make autonomous detection decisions. Machine Learning (ML) algorithms such as Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), and Decision Trees have been widely applied for intrusion classification. While these methods improve detection accuracy compared to static rule-based systems, they often face challenges related to high-dimensional datasets, computational complexity, and the need for extensive feature engineering.

More advanced ensemble learning techniques have demonstrated improved performance in handling structured cybersecurity datasets. Algorithms such as Extreme Gradient Boosting (XGBoost) enhance predictive accuracy through

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802039

iterative error correction and optimized feature selection. These models are capable of processing large volumes of network traffic data, system logs, and user behavior records while maintaining computational efficiency. However, ensuring model interpretability and reducing false positive rates remain critical considerations for practical deployment in SME environments.

To address these challenges, this research proposes a hybrid AI-driven Intrusion Detection System tailored for SME networks. The system integrates structured data preprocessing with an XGBoost-based classification model to achieve improved detection accuracy and adaptability. The study focuses on designing, implementing, and evaluating the proposed framework, emphasizing performance enhancement, scalability, and real-time applicability in evolving cybersecurity landscapes.

II. LITERATURE REVIEW

The application of Artificial Intelligence (AI) in Intrusion Detection Systems (IDS) has become a major research focus due to the increasing sophistication of cyber threats. Early IDS frameworks primarily relied on traditional Machine Learning (ML) algorithms such as Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), and Decision Trees to classify network traffic and detect malicious behavior. These approaches demonstrated improved detection accuracy compared to signature-based systems; however, they often required extensive feature engineering and faced performance degradation when handling high-dimensional and large-scale network datasets.

With the advancement of computational capabilities, ensemble learning and Deep Learning (DL) techniques have been introduced to enhance IDS performance. Convolutional Neural Networks (CNNs) have been utilized for extracting spatial features from traffic data, while Long Short-Term Memory (LSTM) networks have been employed to capture sequential and temporal attack patterns. Although these models achieved high detection accuracy, their computational complexity and lack of interpretability limited their deployment in resource-constrained environments such as Small and Medium Enterprises (SMEs). The “black-box” nature of deep learning models also raises concerns regarding transparency and trust in security-critical applications.

To improve both performance and efficiency, researchers have increasingly explored ensemble-based algorithms such as Random Forest and Extreme Gradient Boosting (XGBoost). These models combine multiple decision trees to enhance classification robustness while reducing overfitting. XGBoost, in particular, has demonstrated superior performance in structured cybersecurity datasets due to its gradient boosting mechanism, regularization capability, and efficient handling of missing or imbalanced data. Compared to deep learning architectures, ensemble models offer a balance between accuracy, computational efficiency, and interpretability.

Recent studies also highlight the importance of Explainable AI (XAI) for improving model transparency and supporting decision-making in operational environments. Additionally, data scarcity and imbalance remain critical challenges in IDS research, prompting the use of synthetic data generation and advanced feature selection techniques. Despite significant advancements, issues related to real-time implementation, scalability, and false positive reduction continue to drive ongoing research in AI-powered IDS frameworks.

III. RESEARCH METHODOLOGY

This study adopts an experimental research methodology to design and evaluate a hybrid AI-driven Intrusion Detection System (IDS) tailored for Small and Medium Enterprise (SME) network environments. The objective is to develop a machine learning-based detection framework capable of accurately classifying normal and malicious network activities while maintaining computational efficiency suitable for practical deployment.

The proposed methodology consists of structured data collection, preprocessing, model training, and performance evaluation phases. Network traffic logs, system activity records, and login behavior data were used as input features for the detection model. The dataset was divided into training (70%) and testing (30%) subsets to ensure unbiased model validation. Data preprocessing techniques, including cleaning, normalization, and feature selection, were applied to remove inconsistencies and improve classification accuracy.

The core detection mechanism is based on the Extreme Gradient Boosting (XGBoost) algorithm, an ensemble learning technique that enhances predictive performance through iterative gradient optimization and error minimization. XGBoost was selected due to its ability to handle structured datasets efficiently, prevent overfitting through

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802039

regularization, and manage high-dimensional feature spaces effectively. The model was trained to classify network behavior into normal and intrusion categories based on extracted traffic and system features.

Performance evaluation was conducted using standard metrics such as accuracy, R^2 score, and comparative improvement over conventional IDS techniques. A comparative analysis was performed to assess the effectiveness of the proposed model in reducing false positives and improving detection rates. The experimental findings were analyzed to determine the suitability of the hybrid AI-driven IDS for real-time SME cybersecurity applications.

IV. RESULTS AND DISCUSSION

The experimental evaluation of the proposed AI-driven Intrusion Detection System (IDS) demonstrates significant improvement in detection performance compared to conventional IDS approaches. The XGBoost-based hybrid model was trained and tested using structured network traffic and system activity datasets, enabling accurate classification of normal and malicious behaviors. The ensemble learning mechanism effectively optimized feature importance and minimized classification errors through iterative gradient boosting. The proposed model achieved a detection accuracy of 96%, outperforming traditional IDS techniques that achieved 89% accuracy under the same experimental conditions. The improvement of approximately 6% highlights the effectiveness of gradient boosting in handling structured cybersecurity datasets. Additionally, the R^2 score showed measurable enhancement, indicating better predictive consistency and model reliability. The results confirm that ensemble-based machine learning models can significantly reduce misclassification rates and improve intrusion detection robustness.

A key advantage of the XGBoost algorithm lies in its ability to manage high-dimensional feature spaces while preventing overfitting through built-in regularization mechanisms. Feature selection and preprocessing further contributed to improved detection performance by eliminating redundant attributes and enhancing relevant traffic characteristics. The model demonstrated stable classification behavior across both training and testing datasets, indicating strong generalization capability.

Compared to deep learning architectures, the proposed ensemble model maintains lower computational complexity while achieving competitive accuracy. This makes it particularly suitable for Small and Medium Enterprise (SME) environments where computational resources may be limited. However, challenges remain in optimizing real-time deployment and minimizing false positives under large-scale network conditions.

Overall, the experimental results validate that the integration of XGBoost within a hybrid IDS framework enhances detection accuracy, computational efficiency, and adaptability. The findings support the feasibility of deploying AI-driven IDS solutions in practical SME cybersecurity infrastructures while maintaining balanced performance and scalability.

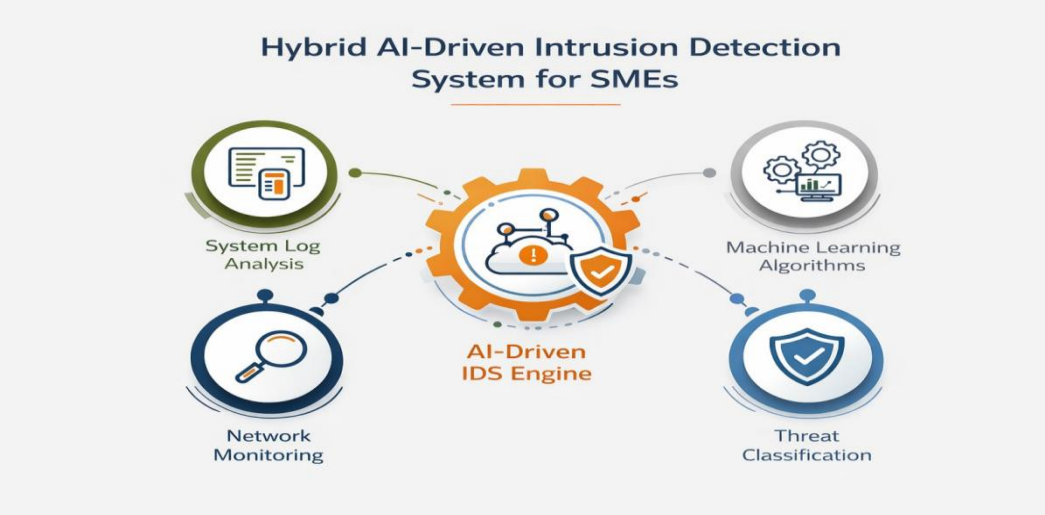

FIG: 1

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802039

V. CONCLUSION

The proposed Hybrid AI-driven Intrusion Detection System demonstrates the effectiveness of machine learning techniques in enhancing cybersecurity for Small and Medium Enterprise (SME) environments. By leveraging the Extreme Gradient Boosting (XGBoost) algorithm, the system achieves improved detection accuracy, reduced false positives, and enhanced classification reliability compared to conventional IDS approaches.

The integration of structured data preprocessing, feature optimization, and ensemble learning mechanisms enables the model to efficiently analyze network traffic patterns and system activity logs. Unlike traditional signature-based systems, the proposed framework provides adaptive and data-driven threat detection, making it more resilient against evolving and previously unseen cyberattacks. The experimental results validate that ensemble-based AI models offer a balanced combination of accuracy, computational efficiency, and scalability.

Despite the promising results, certain challenges remain, including optimizing real-time deployment, managing large-scale network data, and maintaining consistent performance under dynamic threat conditions. Continuous model updates and system monitoring are necessary to ensure sustained effectiveness in rapidly changing cybersecurity landscapes.

In conclusion, the Hybrid AI-driven IDS presents a practical and intelligent solution for strengthening SME network security. The findings highlight the potential of ensemble machine learning approaches in building adaptive, efficient, and reliable intrusion detection systems for modern digital infrastructures.

VI. FUTURE WORK

1. **Lightweight and Scalable Model Optimization:** Future work can explore the development of optimized and lightweight ensemble models suitable for deployment in resource-constrained SME networks and edge-based environments. Reducing computational overhead while maintaining high detection accuracy will be essential for real-time applications.
2. **Real-Time Deployment and Streaming Analysis:** Implementing the proposed XGBoost-based IDS within live network environments using real-time traffic streaming frameworks can enhance practical applicability. This includes optimizing response latency and improving continuous monitoring capabilities.
3. **Online and Incremental Learning:** Integrating adaptive learning mechanisms that allow the model to update dynamically with new traffic patterns can improve resilience against emerging and zero-day attacks without requiring complete retraining.
4. **Enhanced Explainability and Feature Transparency:** Incorporating explainable AI techniques to analyze feature importance and model decisions can improve transparency and assist security administrators in understanding intrusion patterns more effectively.
5. **Handling Imbalanced and Large-Scale Data:** Advanced feature selection, data balancing strategies, and synthetic data generation techniques can be explored to enhance robustness against rare attack categories.
6. **Integration with Threat Intelligence Systems:** Future systems may combine the IDS framework with external threat intelligence feeds to enrich contextual awareness and improve proactive threat detection.
7. **Security Against Adversarial Manipulation:** Research can also focus on strengthening the IDS against adversarial attacks designed to bypass machine learning-based detection mechanisms.

REFERENCES

1. Y. Zhang, X. Li, and H. Wang, “Hybrid CNN-LSTM Model for Intrusion Detection in IoT Networks,” *IEEE Transactions on Information Forensics and Security*, vol. 19, no. 1, pp. 112–124, 2024.
2. S. Kim and J. Park, “Generative Adversarial Networks for Synthetic Attack Data Augmentation in Intrusion Detection Systems,” *Journal of Cybersecurity and Privacy*, vol. 3, no. 2, pp. 45–60, 2024.
3. A. Singh and R. Gupta, “Explainable AI in Intrusion Detection: Techniques and Applications,” *ACM Computing Surveys*, vol. 56, no. 4, Article 89, 2024.
4. L. Chen and F. Zhao, “Reinforcement Learning-Based Adaptive Firewall for Real-Time Intrusion Mitigation,” *IEEE Access*, vol. 12, pp. 67890–67902, 2024.
5. C.Nagarajan and M.Madheswaran - ‘Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques’- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802039

6. C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2
7. C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9
8. S.Tamilselvi, R.Prakash, C.Nagarajan,"Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller" Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025
9. S.Tamilselvi, R.Prakash, C.Nagarajan," Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance" Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
10. S.Thirunavukkarasu, C. Nagarajan, 2024, "Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
11. C. Nagarajan, M.Madheswaran and D.Ramasubramanian- 'Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model'- Acta Electrotechnica et Informatica Journal , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.
12. C.Nagarajan and M.Madheswaran - 'DSP Based Fuzzy Controller for Series Parallel Resonant converter'- Springer, Frontiers of Electrical and Electronic Engineering, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.
13. C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
14. C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
15. Suganthi Mullainathan, Ramesh Natarajan, "An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques", Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
16. M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
17. T. Wang and Y. Liu, "Federated Learning for Privacy-Preserving Intrusion Detection in Industrial Cyber-Physical Systems," *Computers & Security*, vol. 118, p. 102796, 2024.
18. M. Patel and P. Shah, "Robust Intrusion Detection Against Adversarial Attacks: A Survey," *Information Sciences*, vol. 612, pp. 367–387, 2024.