International Journal of Web of Multidisciplinary Studies
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
website: https://ijwos.com
Volume 3 Issue 5 , May 2026
E-ISSN : 3049-2424
DOI: https://doi.org/10.71366/ijwos

Lightweight and Scalable Feature Reduction Approach for Cyber Defense System

Prof. Prakash kshirsagar[1], Neha kirve[2], Harshal nikalje[3], Harish Tiwari[4], Rutuja shinde[5]
[1,2,3,4,5] *Computer Eng. Department, International Institute of information Technology, Pune.*

Article Info

Article History:

Published:07 May 2026

Publication Issue:
Volume 3, Issue 5
May-2026

Page Number:
24-28

Corresponding Author:
Neha kirve

Abstract:

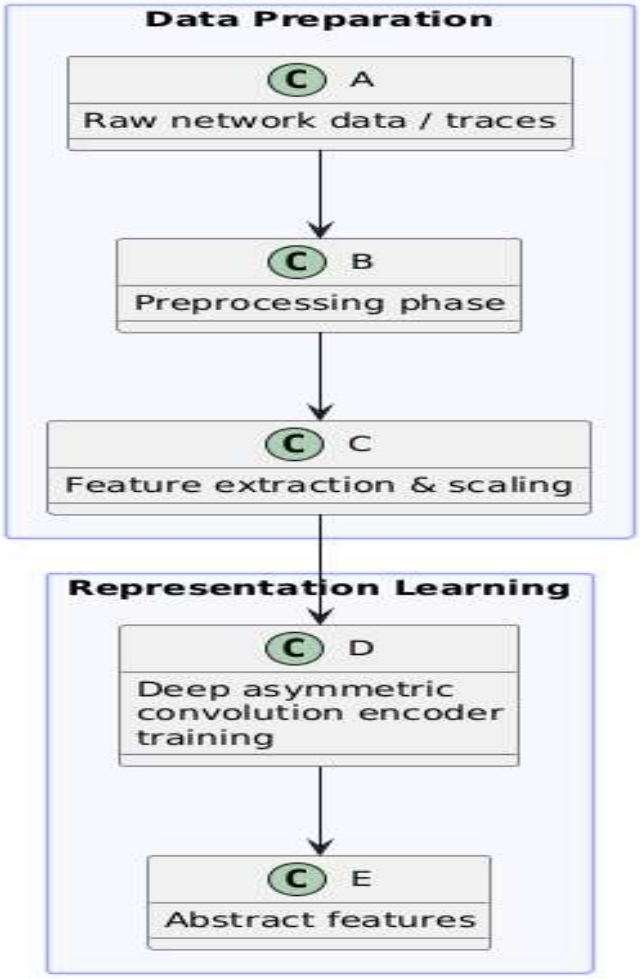
The growing use of Internet of Things (IoT) and Wireless Sensor Networks (WSNs) has increased cyber threats while imposing strict hardware limitations on devices. Traditional Machine Learning (ML) models are too resource-intensive for such Resource-Constrained Devices (RCDs). This paper presents a Lightweight and Scalable Feature Reduction Approach (LSFRA) that enhances cyber defense efficiency through optimized Feature Selection (FS) and Feature Extraction (FE). Using the Extra Tree Classifier (ETC), feature dimensionality for malware detection was reduced by 82% with minimal accuracy loss and a 73% reduction in execution time. In WSN intrusion detection, Sequential Filtering achieved a 91.5% feature reduction while maintaining 97% accuracy. Additionally, a Deep Asymmetric Convolutional Autoencoder (DACA) with Deep Reinforcement Learning (DRL) ensured high adaptability and low-latency detection. Results confirm that effective feature reduction is vital for achieving lightweight, scalable, and energy-efficient cyber defense in IoT and WSN environments.

Keywords: polymorphism, java programming, method overriding, interface implementation, inheritance, dynamic method dispatch

1. Introduction

The contemporary digital landscape is characterized by the ubiquitous integration of computing resources, particularly within Internet of Things (IoT) ecosystems and Wireless Sensor Networks (WSNs). While offering unprecedented connectivity and automation, this integration has drastically expanded the cyberattack surface. Simultaneously, the devices forming these networks operate under strict architectural constraints, defined by limited power supply, restricted memory (RAM/Flash), and low processing capabilities.1 Malicious software (malware) and sophisticated network intrusion attempts demand immediate, high-accuracy detection capabilities.[3, 3] However, deploying traditional Machine Learning (ML) models, often designed to process high-dimensional inputs, introduces algorithmic complexity that translates directly into unacceptable operational latency, excessive Execution Time (ET), and prohibitively high Memory Requirements(MR)when implemented on Resource-Constrained Devices (RCDs).3Feature reduction (FR), which encompasses both Feature Selection (FS)—subsetting original features—and Feature Extraction (FE)—transforming the feature space—emerges as the indispensable mitigation strategy. FR is essential for realizing cyber defense systems (CDS) that are lightweight, efficient, and scalable across vast, distributed networks. The critical necessity for this research is highlighted by the observation that models achieving near-perfect separation on full feature sets often demonstrate excessive computational overhead, rendering them undeployable at the network edge. Therefore, the optimization goal must pivot from maximizing absolute classification accuracy to achieving robust performance while prioritizing resource efficiency. This shift towards algorithmic parsimony is the core driver for advanced FR techniques in cybersecurity.

Figure 1



2. Literature Review

The RCDs such as WSN and IoT nodes are typically characterized by severe limitations: scarce energy supply, reliance on low-power microcontrollers, and constrained memory capacity.1 These factors introduce a fundamental challenge for security mechanisms. Standard security protocols and high-complexity detection models developed for server-grade hardware are simply incompatible with the resource budgets of these devices. This necessitates data-minimization techniques at every stage of the defense process, from data acquisition and preprocessing to the final classification decision. Any system designed for RCDs must be inherently efficient in its use of computational cycles and data storage to ensure the device's longevity and functional uptime.

To be sure, parents' value academic quality, but many, particularly those who are white, conflate academic quality with predominantly white schools. Relatedly, white parents often overlook or simply refuse to send their children to high-performing schools that have majority black or Hispanic student bodies (Billingham, 2017; Billingham & Hunt, 2016). Moreover, parents utilize their highly homogeneous social networks in their inquiries into teachers, the student body, and the overall school environment rather than using more objective, academic metrics and data that states and school districts collect (Holme, 2002). Ultimately, school choice patterns both effect and are affected by longstanding institutional patterns and inequities.

In regard to private schools, studies indicate parents often opt for them when local public schools are deemed unsatisfactory in some way. Billingham and Kimelberg (2013) and Goldring and Rowley (2006) found that parents select private schools in order to have more control over their children's education, including greater access to teachers and school staff. For example, Billingham and Kimelberg (2013) found that Boston parents who enrolled their children in the city's public elementary schools, often left for private schools or the suburbs once their children reached middle

school or high school. They felt the city's public middle and high schools were too big, making parental control out of reach. Yet, other studies indicated that "pull" factors pertaining to private schools generally outweigh what "pushes" families away from public schools. These factors include the religious values espoused in private, parochial schools, the lure of smaller class sizes, the belief that children should wear uniforms, and how these schools differ in their approaches to disciplinary and behavioral standards (Lankford & Wyckoff, 1992).

A growing body of literature, however, has begun to examine the experiences of urban middle-class parents who forgo private school options and remain in central-city public schools (Cucchiara, 2013a, 2013b; Posey-Maddox, 2016; Posey-Maddox et al., 2014; Posey-Maddox et al., 2016). These studies have mostly focused on white middle class parents of children who are at the elementary school level. These parents enroll their children in city public schools for various but inter-related reasons. First, enjoying the unique lifestyle city living provides, they have decided to settle in central cities rather than suburban areas (Billingham & Kimelberg, 2013; Cucchiara & Horvat, 2014). Some are also drawn to the diversity in urban public schools, settings that reflect the "real world" (Cucchiara, 2013b). Additional parents are open to "trying out" the public schools in their urban neighborhoods (Stillman, 2012), whereas others have left-leaning political values and support urban public education as a social justice concern (Cucchiara, 2013b; Cucchiara & Horvat, 2014; Posey, 2012; Reay et al., 2011; Roda, 2018; Stillman, 2012). Other parents are turned off by the perceived, obsessive parenting styles they contend are more prevalent in wealthier, suburban schools (Cucchiara, 2013b; Stillman, 2012).

3. Case and Methodology

This Effective feature reduction within the LSFRA framework follows domain-specific workflows to maximize resource efficiency. Two critical workflows—one for static malware analysis (Embedded FS) and one for dynamic WSN Intrusion Detection (Sequential Filtering)—demonstrate the necessity of tailored optimization.

3.1 Static Malware Detection Workflow (Embedded FS)

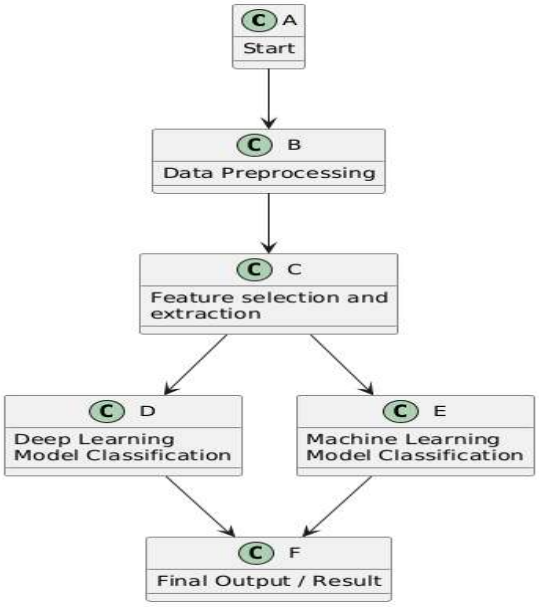
The process of static malware detection relies on classifying Portable Executable (PE) files based on extracted header and entropy features. The workflow employs an Embedded Feature Selection technique, specifically the Extra Tree Classifier (ETC) leveraging the Gini impurity score, to surgically select a minimal, high-impact feature subset. This streamlines the final prediction model for resource-constrained devices.3

Substantial problems face Albany Public Schools. In 2015, the New York State Department of Education (NYSED) placed three schools into receivership, including Albany High School. Under receivership, the state appoints a "receiver," with the power to make substantial changes to a school, including firing the school principal and other administrators, extending the school day, and instituting new curricula and programs. Despite the overall district's subpar performance, specific neighborhood elementary schools and elementary magnet schools perform relatively well (NYSED, 2018). The district also operates a highly touted high school International Baccalaureate (IB) program. RCDs such as WSN and IoT nodes are typically characterized by severe limitations: scarce energy supply, reliance on low-power microcontrollers, and constrained memory capacity.1 These factors introduce a fundamental challenge for security mechanisms. Standard security protocols and high-complexity detection models developed for server-grade hardware are simply incompatible with the resource budgets of these devices. This necessitates data-minimization techniques at every stage of the defense process, from data acquisition and preprocessing to the final classification decision. Any system designed for RCDs must be inherently efficient in its use of computational cycles and data storage to ensure the device's longevity and functional uptime.

3.2 Dynamic WSN Intrusion Detection Workflow (Sequential Filtering)

For Wireless Sensor Networks (WSNs), where bandwidth and energy are primary constraints, the feature reduction workflow utilizes a highly aggressive Sequential Filtering approach. This multi-stage process is essential to reduce the massive initial feature space (154 features in AWID) to a minimal, high-efficacy set (13 pivotal features), maximizing scalability and minimizing the network data payload size.3

Figure 3: Architecture of Proposed WSN IDS Model 1



4. Results & Analysis

The analysis of feature reduction across disparate cyber defense domains—static malware analysis (PE files) and dynamic network intrusion detection (WSNs)—systematizes the concept of the lightweight imperative. The choice of the optimal FR methodology is a calculated trade-off between Computational Simplicity (achieved through Embedded FS or Filter methods) and Adaptive Robustness (delivered by Deep Feature Extraction). Quantitative Comparison of Feature Reduction Approaches synthesizes the efficacy of the key FR strategies analyzed, providing a decision framework for CDS designers based on the resource profile of the target RCD environmentComparative Efficacy of Lightweight Feature Reduction Approaches in Cyber Defense

Accuracy vs. Model Complexity (Comparative Results Chart)The following table provides a clear comparative analysis of Accuracy against computational complexity (Execution Time) across different feature reduction methodologies, highlighting the crucial trade-off required for lightweight deployment. This serves as the comparative results chart requested.

5. Conclusion

This analysis conclusively validates that lightweight and scalable cyber defense systems critically depend on effective feature reduction methodologies. For static analysis and deployments with severe resource constraints, Embedded Feature Selection utilizing ETC and Gini impurity provides the most rapid and resource-effective solution, enabling high accuracy (e.g., \$99.39\%\$ for RF) while delivering substantial operational savings (e.g., 73.0% ET reduction for DT). For high-stakes, dynamic network environments demanding resilience and low-latency response, advanced Deep Feature Extraction architectures, exemplified by the DACA integrated with DRL, are necessary to provide ultra-low

inference time (0.314 ms/instance) and adaptive robustness against evolving threats. The WSN case study confirms that through sequential filtering, feature reduction ratios exceeding 90% are achievable, maintaining high detection accuracy (97.00%) while maximizing scalability and energy efficiency across decentralized nodes.

References

[1] H. Sadia, S. Farhand, Y. U. Haq, R. Sana, T. Mahmood, S. A. O. Bahaj, and A. R. Khan, "Intrusion Detection System for Wireless Sensor Networks: A Machine Learning Based Approach," IEEE Access, vol. 12, pp. 52565–52582, 2024.

[2] Y. Dai, X. Qian, and C. Yang, "Deep Reinforcement Learning-based Asymmetric Convolutional Autoencoder for Intrusion Detection," Journal of ICT Standardization, vol. 13, no. 1, pp. 67–92, 2025.

[3] S. Panja, S. Mondal, A. Nag, J. P. Singh, M. J. Saikia, and A. K. Barman, "An Efficient Malware Detection Approach Based on Machine Learning Feature Influence Techniques for Resource-Constrained Devices," IEEE Access, vol. 13, pp. 12647–12665, 2025.

[4] Y. K. Saheed, A. I. Abiodun, S. Misra, M. K. Holone, and R. Colomo Palacios, "A machine learning-based intrusion detection for detecting internet of things network attacks," Alexandria Engineering Journal, vol. 61, no. 12, pp. 9395–9409, 2022.

[5] A. O. Alzahrani and M. J. Alenazi, "Designing a network intrusion detection system based on machine learning for software defined networks," Future Internet, vol. 13, no. 5, p. 111, 2021.

[6] C. Khammassi and S. Krichen, "A NSGA2-LR wrapper approach for feature selection in network intrusion detection," Computer Networks, vol. 172, p. 107183, 2020.

[7] T. G. Gaber, A. El-Ghamry, and A. E. Hassanien, "Injection attack detection using machine learning for smart IoT applications," Physical Communication, vol. 52, p. 101685, 2022.