JOURNAL OF SOUTHERN COMMUNICATION ENGINEERING
ISLAMIC AZAD UNIVERSITY BUSHEHR BRANCH

E-ISSN: 2980-9231
https://sanad.iau.ir/journal/jce

https://doi.org/...

Vol. x/ No. x/xxx

Research Article

An Edge-Aware Learning Framework for IoT Malware Classification Using Block-Average-Based Adaptive Dimensionality Reduction

Shohreh Ajoudanian[1, 3] | Maryam Nooraei Abadeh[2]

[1]Department of Computer Engineering, Na.C., Islamic Azad University, Najafabad, Iran.
shajoudanian@iau.ac.ir

[2]Department of Computer Engineering, Arv. C., Islamic Azad University, Abadan, Iran
ma.nooraei@iau.ac.ir

[3]Big Data Research Center, Na.C., Islamic Azad University, Najafabad, Iran.

Correspondence
Shohreh Ajoudabnian, Assistant Professor of Computer Engineering, Na.C., Islamic Azad University, Najafabad, Iran.
Email: shajoudanian@iau.ac.ir

Main Subject:
IoT

History:
Received: 16 March 2025
Revised: 27 April 2025
Accepted: 7 May 2025

Abstract

With the rapid expansion of the Internet of Things (IoT), the number of connected devices has surged, bringing significant challenges in both cybersecurity and large-scale data processing. One of the main challenges is detecting newly emerging malware, which often goes unnoticed by traditional signature-based detection methods. Machine learning has been introduced as a promising solution for classifying IoT malware. However, implementing these models directly on IoT devices is difficult due to limitations in processing power, memory, and energy resources. To overcome these issues, this paper presents an edge-aware learning framework that incorporates an adaptive block-averaged dimensionality reduction technique. This approach enables data to be processed locally on edge devices, reducing the need to transmit large volumes of raw data to cloud servers. Consequently, the framework significantly reduces processing latency, accelerates threat detection, and increases efficiency in environments with limited resources. The adaptive dimensionality reduction method effectively compresses feature data while preserving essential information. This not only improves the performance and accuracy of machine learning models but also decreases energy consumption. In summary, the proposed solution enables the deployment of secure, high-performance, real-time malware detection systems in IoT ecosystems, thereby enhancing overall system efficiency and ensuring better protection against evolving threats.

Keywords: Block Average-Based Dimensionality Reduction, Edge Processing, Internet of Things, Malware Classification, Machine Learning.

Highlights

- Introducing the Adaptive Block Matrix Dimensionality Reduction (ABMD) method for IoT data processing with high accuracy and preserved critical information.
- Designing an integrated architecture for raw IoT data analysis and malware detection using machine learning.
- Utilizing optimization algorithms for machine learning models such as LGBM and RF to enhance accuracy and reduce processing time.

Citation: [in Persian].

1. Introduction

The rapid growth of Internet of Things (IoT) systems has led to an exponential increase in data generation, creating significant challenges for efficient data processing and security management. Traditional malware detection methods, such as signature-based approaches, often fail to identify new and evolving threats in these environments [1]. The high dimensionality of IoT data also adds complexity, making it difficult to maintain system efficiency and accuracy [2]. Recent studies have emphasized the importance of feature reduction techniques to enhance computational efficiency and system reliability in IoT networks [1, 3]. To address these challenges, this paper introduces an innovative feature reduction method based on Adaptive Block Mean Division (ABMD). This method ensures the preservation of critical information while minimizing noise, enabling IoT systems to process data more efficiently. By integrating ABMD with machine learning models, the proposed approach improves key performance metrics, including accuracy, recall, and F1-score, in malware detection tasks. Additionally, the method demonstrates its effectiveness in handling unknown threats and optimizing data processing in distributed IoT environments, paving the way for more secure and efficient IoT systems [1, 3].

2. Innovation and contributions

This paper introduces a novel framework to address the challenges of malware detection and classification in resource-constrained IoT environments. The proposed method utilizes an Adaptive Block Mean Division (ABMD) technique for feature reduction, which effectively minimizes data dimensionality while preserving critical information. This approach not only reduces noise but also optimizes the performance of IoT devices, making it well-suited for low-power and resource-limited systems. Furthermore, an edge-aware learning framework is presented, enabling on-device malware classification and reducing dependency on cloud-based systems, which significantly enhances response times. The method is evaluated on real-world IoT datasets, demonstrating its ability to detect and classify unknown malware with high accuracy and efficiency. Additionally, the study compares the performance of various machine learning models, including Logistic Regression, Random Forest, and LightGBM, highlighting the effectiveness of the proposed approach in improving performance metrics such as accuracy, recall, and F1-score. By bridging the gap between traditional malware detection methods and the growing need for lightweight, efficient solutions, this study offers a scalable and practical framework for enhancing security in distributed IoT systems.

3. Materials and Methods

The study leverages the BODMAS dataset, which includes 134,435 samples comprising 57,293 malware and 77,142 benign Windows PE files collected between August 2019 and September 2020. Each sample is represented by 2,381 features, encompassing non-destructive metadata, binary information, and other attributes crucial for malware detection. To address the challenge of high-dimensional data, the Adaptive Block Mean Division (ABMD) method is employed for feature reduction, which effectively eliminates noise and reduces dimensionality while preserving essential information.

Following the feature reduction process, multiple machine learning models, such as Logistic Regression (LR), Random Forest (RF), k-Nearest Neighbors (k-NN), LightGBM (LGBM), and Linear Discriminant Analysis (LDA), are trained and evaluated to classify malware. The models are validated using k-fold cross-validation techniques to ensure robustness and generalizability. The proposed approach also incorporates edge-aware processing to optimize performance within IoT environments, allowing for efficient on-device classification and reducing dependency on centralized systems. This combination of advanced feature reduction and machine learning algorithms ensures a scalable and efficient solution for malware detection and classification.

4. Results and Discussion

The results of this study demonstrate the effectiveness of the Adaptive Block Mean Division (ABMD) technique in reducing data dimensionality and noise while preserving essential features for malware detection and classification. The proposed method significantly improved the performance of machine learning models across several evaluation metrics, including accuracy, recall, F1-score, and processing efficiency. Among the tested models, LightGBM (LGBM) and Random Forest (RF) achieved the highest overall performance, with LGBM demonstrating superior accuracy and F1-score in most scenarios.

Comparative analysis with other feature reduction methods, such as Principal Component Analysis (PCA) and SKBF, revealed that ABMD consistently outperformed these approaches by maintaining higher recall and precision rates. For instance, ABMD achieved an F1-score of 0.915 in the Logistic Regression model, which was higher than the scores obtained by PCA and SKBF. Additionally, ABMD proved to be highly effective in handling complex and unknown threats, showcasing its adaptability in dynamic IoT environments.

Furthermore, the edge-aware learning framework integrated with ABMD demonstrated significant improvements in response times, making it suitable for real-time malware detection in IoT devices. The study also highlighted the role of feature reduction in minimizing computational load, which is critical for resource-constrained IoT

systems. Overall, the proposed approach not only enhances detection accuracy but also provides a scalable and efficient solution for improving IoT system security.

5. Conclusion

This study introduced a novel framework for malware detection and classification in IoT environments, addressing the critical challenges of high-dimensional data and resource constraints. By employing the Adaptive Block Mean Division (ABMD) technique for feature reduction, the proposed method successfully minimized noise and preserved essential information, leading to significant improvements in accuracy, recall, and F1-score across multiple machine learning models. Among the evaluated models, LightGBM and Random Forest demonstrated superior performance, highlighting the effectiveness of the proposed approach.

The integration of edge-aware processing further enhanced the system's efficiency by enabling real-time classification and reducing dependence on centralized systems, making the framework ideal for dynamic and resource-constrained IoT environments. Comparative analysis with other feature reduction methods showed that ABMD consistently outperformed traditional approaches like PCA and SKBF, establishing its robustness and adaptability.

In conclusion, the proposed framework bridges the gap between conventional malware detection methods and the growing need for lightweight, efficient solutions tailored for IoT systems. It provides a scalable, reliable, and effective solution for improving security in distributed environments, paving the way for future research and applications in IoT security.

6. Acknowledgement

The authors appreciate the efforts of all colleagues and collaborators who assisted in data collection, analysis, and validation, enabling the successful completion of this study.

References

[1] e. a. Alasmary H, "Analyzing and detecting emerging Internet of Things malware: a graph-based approach," *IEEE Internet Things J,* 2019.

[2] W. K. Ali I, Bayomi H. , "Dimensionality reduction for images of IoT using machine learning," 2024, doi: 10.1038/s41598-024-57385-4. .

[3] R. Ghadiri, "Security and Performance Analysis of Edge Computing in IoT," 2023.

Declaration of Competing Interest: Authors do not have conflict of interest. The content of the paper is approved by the authors.

Author Contributions:

Shohreh Ajoudanian: Methodology, writing original draft preparation; **Maryam Nooraei Abadeh**: Resources, methodology, manuscript editing.